US011423641B2

(12) **United States Patent**
Ross et al.

(10) **Patent No.: US 11,423,641 B2**
(45) **Date of Patent: *Aug. 23, 2022**

(54) **DATABASE FOR DETECTING COUNTERFEIT ITEMS USING DIGITAL FINGERPRINT RECORDS**

(71) Applicant: **Alitheon, Inc.**, Bellevue, WA (US)

(72) Inventors: **David Justin Ross**, Bellevue, WA (US); **Brian J. Elmenhurst**, Bellevue, WA (US); **Mark Tocci**, Bellevue, WA (US); **John Forbes**, Bellevue, WA (US); **Heather Wheelock Ross**, Bellevue, WA (US)

(73) Assignee: **Alitheon, Inc.**, Bellevue, WA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 93 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **17/102,115**

(22) Filed: **Nov. 23, 2020**

(65) **Prior Publication Data**

US 2021/0103760 A1 Apr. 8, 2021

Related U.S. Application Data

(60) Continuation of application No. 15/862,556, filed on Jan. 4, 2018, now Pat. No. 10,872,265, which is a (Continued)

(51) **Int. Cl.**
G06V 10/75 (2022.01)
G06T 7/00 (2017.01)
(Continued)

(52) **U.S. Cl.**
CPC ***G06V 10/751*** (2022.01); ***G06T 1/005*** (2013.01); ***G06T 7/0004*** (2013.01); ***G06V 10/225*** (2022.01); ***G06V 10/245*** (2022.01); ***G06V 10/478*** (2022.01); ***G06V 20/46*** (2022.01); ***G06V 30/412*** (2022.01); ***G09C 5/00*** (2013.01);
(Continued)

(58) **Field of Classification Search**
USPC 382/100, 305
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,218,674 A 8/1980 Brosow et al.
4,423,415 A 12/1983 Goldman
(Continued)

FOREIGN PATENT DOCUMENTS

DE 102006005927 A1 8/2007
EP 0439669 A2 8/1991
(Continued)

OTHER PUBLICATIONS

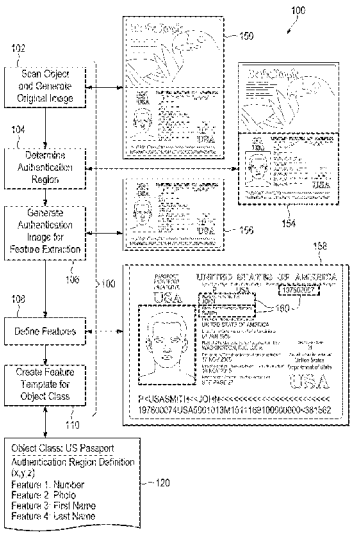
Stern et al., EMFORCED: EM-Based Fingerprinting Framework for Remarked and Cloned Counterfeit IC Detection Using Machine Learning Classification, 1063-8210 2019 IEEE, pp. 363-375. (Year: 2020).*
(Continued)

Primary Examiner — Ishrat I Sherali
(74) *Attorney, Agent, or Firm* — Cozen O'Connor

(57) **ABSTRACT**

Improvements are disclosed for detecting counterfeit objects, based on comparison to digital fingerprints that describe features found in images of objects known to be counterfeit.

21 Claims, 14 Drawing Sheets



Related U.S. Application Data

continuation of application No. 15/208,339, filed on Jul. 12, 2016, now Pat. No. 10,192,140, which is a division of application No. 14/531,724, filed on Nov. 3, 2014, now Pat. No. 9,443,298, which is a continuation-in-part of application No. 14/290,653, filed on May 29, 2014, now Pat. No. 9,350,552, which is a continuation of application No. 13/410,753, filed on Mar. 2, 2012, now Pat. No. 8,774,455.

(60) Provisional application No. 61/448,465, filed on Mar. 2, 2011, provisional application No. 61/914,722, filed on Dec. 11, 2013, provisional application No. 61/898,780, filed on Nov. 1, 2013.

(51) **Int. Cl.**

G06T 1/00	(2006.01)
H04L 9/32	(2006.01)
G09C 5/00	(2006.01)
G06V 10/22	(2022.01)
G06V 10/24	(2022.01)
G06V 10/46	(2022.01)
G06V 20/40	(2022.01)
G06V 30/412	(2022.01)
G06Q 50/32	(2012.01)

(52) **U.S. Cl.**

CPC ***H04L 9/3247*** (2013.01); *G06Q 50/32* (2013.01); *G06T 2201/0065* (2013.01); *G06T 2207/30128* (2013.01); *G06T 2207/30144* (2013.01); *G06T 2207/30148* (2013.01); *G06T 2207/30164* (2013.01); *G06T 2207/30204* (2013.01)

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,677,435	A	6/1987	Causse et al.
4,700,400	A	10/1987	Ross
4,883,971	A	11/1989	Jensen
4,921,107	A	5/1990	Hofer
5,031,223	A	7/1991	Rosenbaum et al.
5,079,714	A	1/1992	Manduley et al.
5,393,939	A	2/1995	Nasuta et al.
5,422,821	A	6/1995	Allen et al.
5,514,863	A	5/1996	Williams
5,518,122	A	5/1996	Tilles et al.
5,521,984	A	5/1996	Denenberg et al.
5,703,783	A	12/1997	Allen et al.
5,719,939	A	2/1998	Tel
5,734,568	A	3/1998	Borgendale et al.
5,745,590	A	4/1998	Pollard
5,883,971	A	3/1999	Bolle et al.
5,923,848	A	7/1999	Goodhand et al.
5,974,150	A	10/1999	Kaish et al.
6,205,261	B1	3/2001	Goldberg
6,246,794	B1	6/2001	Kagehiro et al.
6,292,709	B1	9/2001	Uhl et al.
6,327,373	B1	12/2001	Yura
6,343,327	B2	1/2002	Daniels et al.
6,360,001	B1	3/2002	Berger et al.
6,370,259	B1	4/2002	Hobson et al.
6,400,805	B1	6/2002	Brown et al.
6,424,728	B1	7/2002	Ammar
6,434,601	B1	8/2002	Rollins
6,470,091	B2	10/2002	Koga et al.
6,539,098	B1	3/2003	Baker et al.
6,549,892	B1	4/2003	Sansone
6,597,809	B1	7/2003	Ross et al.
6,643,648	B1	11/2003	Ross et al.
6,697,500	B2	2/2004	Woolston et al.
6,741,724	B1	5/2004	Bruce et al.
6,768,810	B2	7/2004	Emanuelsson et al.
6,778,703	B1	8/2004	Zlotnick
6,805,926	B2	10/2004	Cote et al.
6,816,602	B2	11/2004	Coffelt et al.
6,829,369	B2	12/2004	Poulin et al.
6,961,466	B2	11/2005	Imagawa et al.
6,985,925	B2	1/2006	Ogawa
6,985,926	B1	1/2006	Ferlauto et al.
7,016,532	B2	3/2006	Boncyk et al.
7,031,519	B2	4/2006	Elmenhurst
7,096,152	B1	8/2006	Ong
7,120,302	B1	10/2006	Billester
7,121,458	B2	10/2006	Avant et al.
7,152,047	B1	12/2006	Nagel
7,171,049	B2	1/2007	Snapp
7,204,415	B2	4/2007	Payne et al.
7,212,949	B2	5/2007	Bachrach
7,333,987	B2	2/2008	Ross et al.
7,343,623	B2	3/2008	Ross
7,356,162	B2	4/2008	Caillon
7,379,603	B2	5/2008	Ross et al.
7,436,979	B2	10/2008	Bruce et al.
7,477,780	B2	1/2009	Boncyk et al.
7,518,080	B2	4/2009	Amato
7,602,938	B2	10/2009	Prokoski
7,674,995	B2	3/2010	Desprez et al.
7,676,433	B1	3/2010	Ross et al.
7,680,306	B2	3/2010	Boutant et al.
7,720,256	B2	5/2010	Desprez et al.
7,726,457	B2	6/2010	Maier et al.
7,726,548	B2	6/2010	Delavergne
7,748,029	B2	6/2010	Ross
7,822,263	B1	10/2010	Prokoski
7,834,289	B2	11/2010	Orbke et al.
7,853,792	B2	12/2010	Cowburn
8,022,832	B2	9/2011	Vogt et al.
8,032,927	B2	10/2011	Ross
8,108,309	B2	1/2012	Tan
8,180,174	B2	5/2012	Di et al.
8,180,667	B1	5/2012	Baluja et al.
8,194,938	B2	6/2012	Wechsler et al.
8,316,418	B2	11/2012	Ross
8,374,020	B2	2/2013	Katti
8,374,399	B1	2/2013	Talwerdi
8,374,920	B2	2/2013	Hedges et al.
8,391,583	B1	3/2013	Mennie et al.
8,428,772	B2	4/2013	Miette et al.
8,437,530	B1	5/2013	Mennie et al.
8,457,354	B1	6/2013	Kolar et al.
8,477,992	B2	7/2013	Paul et al.
8,520,888	B2	8/2013	Spitzig et al.
8,526,743	B1	9/2013	Campbell et al.
8,774,455	B2	7/2014	Elmenhurst et al.
8,959,029	B2	2/2015	Jones et al.
9,031,329	B1	5/2015	Farid et al.
9,058,543	B2	6/2015	Campbell et al.
9,152,862	B2	10/2015	Ross et al.
9,170,654	B2	10/2015	Boncyk et al.
9,224,196	B2	12/2015	Duerksen et al.
9,234,843	B2	1/2016	Sopori et al.
9,245,133	B1	1/2016	Durst et al.
9,350,552	B2 *	5/2016	Elmenhurst G06F 16/583
9,350,714	B2	5/2016	Freeman et al.
9,361,507	B1	6/2016	Hoyos et al.
9,361,596	B2	6/2016	Ross et al.
9,424,461	B1	8/2016	Yuan et al.
9,443,298	B2	9/2016	Ross et al.
9,558,463	B2	1/2017	Ross et al.
9,582,714	B2	2/2017	Ross et al.
9,646,206	B2	5/2017	Ross et al.
9,665,800	B1	5/2017	Kuffner
9,741,724	B2	8/2017	Seshadri et al.
10,037,537	B2	7/2018	Withrow et al.
10,043,073	B2	8/2018	Ross et al.
10,192,140	B2 *	1/2019	Ross G06V 10/751
10,199,886	B2	2/2019	Li et al.
10,346,852	B2	7/2019	Ross et al.
10,505,726	B1	12/2019	Andon et al.
10,540,664	B2	1/2020	Ross et al.

(56) **References Cited**

U.S. PATENT DOCUMENTS

10,572,883 B2 2/2020 Ross et al.
10,614,302 B2 4/2020 Withrow et al.
10,621,594 B2 4/2020 Land et al.
10,740,767 B2 8/2020 Withrow
10,872,265 B2 * 12/2020 Ross G06T 7/0004
10,936,838 B1 3/2021 Wong
11,238,146 B2 * 2/2022 Ross G06V 20/80
2001/0010334 A1 8/2001 Park et al.
2001/0054031 A1 12/2001 Lee et al.
2002/0015515 A1 2/2002 Lichtermann et al.
2002/0073049 A1 6/2002 Dutta
2002/0134836 A1 9/2002 Cash et al.
2002/0168090 A1 11/2002 Bruce et al.
2003/0015395 A1 1/2003 Hallowell et al.
2003/0046103 A1 3/2003 Amato et al.
2003/0091724 A1 5/2003 Mizoguchi
2003/0120677 A1 6/2003 Vernon
2003/0138128 A1 7/2003 Rhoads
2003/0179931 A1 9/2003 Sun
2003/0182018 A1 9/2003 Snapp
2003/0208298 A1 11/2003 Edmonds
2003/0219145 A1 11/2003 Smith
2004/0027630 A1 2/2004 Lizotte
2004/0101174 A1 5/2004 Sato et al.
2004/0112962 A1 6/2004 Farrall et al.
2004/0218791 A1 11/2004 Jiang et al.
2004/0218801 A1 11/2004 Houle et al.
2004/0250085 A1 12/2004 Tattan et al.
2005/0007776 A1 1/2005 Monk et al.
2005/0038756 A1 2/2005 Nagel
2005/0065719 A1 3/2005 Khan et al.
2005/0086256 A1 4/2005 Owens et al.
2005/0111618 A1 5/2005 Sommer et al.
2005/0119786 A1 6/2005 Kadaba
2005/0125360 A1 6/2005 Tidwell et al.
2005/0131576 A1 6/2005 De et al.
2005/0137882 A1 6/2005 Cameron et al.
2005/0160271 A9 7/2005 Brundage et al.
2005/0169529 A1 8/2005 Owechko et al.
2005/0188213 A1 8/2005 Xu
2005/0204144 A1 9/2005 Mizutani
2005/0251285 A1 11/2005 Boyce et al.
2005/0257064 A1 11/2005 Boutant et al.
2005/0289061 A1 12/2005 Kulakowski et al.
2006/0010503 A1 1/2006 Inoue et al.
2006/0083414 A1 4/2006 Neumann et al.
2006/0109520 A1 5/2006 Gossaye et al.
2006/0131518 A1 6/2006 Ross et al.
2006/0177104 A1 8/2006 Prokoski
2006/0253406 A1 * 11/2006 Caillon G06V 10/40 705/410
2007/0056041 A1 3/2007 Goodman
2007/0071291 A1 3/2007 Yumoto et al.
2007/0085710 A1 4/2007 Bousquet et al.
2007/0094155 A1 4/2007 Dearing
2007/0211651 A1 9/2007 Ahmed et al.
2007/0211964 A1 9/2007 Agam et al.
2007/0230656 A1 10/2007 Lowes et al.
2007/0263267 A1 11/2007 Ditt
2007/0269043 A1 11/2007 Launay et al.
2007/0282900 A1 12/2007 Owens et al.
2008/0005578 A1 1/2008 Shafir
2008/0008377 A1 1/2008 Andel et al.
2008/0011841 A1 1/2008 Self et al.
2008/0013804 A1 1/2008 Moon et al.
2008/0016355 A1 1/2008 Beun et al.
2008/0128496 A1 6/2008 Bertranou et al.
2008/0130947 A1 6/2008 Ross et al.
2008/0219503 A1 9/2008 Di et al.
2008/0250483 A1 10/2008 Lee
2008/0255758 A1 10/2008 Graham et al.
2008/0272585 A1 11/2008 Conard et al.
2008/0290005 A1 11/2008 Bennett et al.
2008/0294474 A1 11/2008 Furka
2009/0028379 A1 1/2009 Belanger et al.
2009/0057207 A1 3/2009 Orbke et al.
2009/0106042 A1 4/2009 Maytal et al.
2009/0134222 A1 5/2009 Ikeda
2009/0154778 A1 6/2009 Lei et al.
2009/0157733 A1 6/2009 Kim et al.
2009/0223099 A1 9/2009 Versteeg
2009/0232361 A1 9/2009 Miller
2009/0245652 A1 10/2009 Bastos
2009/0271029 A1 10/2009 Doutre
2009/0287498 A2 11/2009 Choi
2009/0307005 A1 12/2009 Omartin et al.
2010/0027834 A1 2/2010 Spitzig et al.
2010/0054551 A1 3/2010 Decoux
2010/0070527 A1 3/2010 Chen
2010/0104200 A1 4/2010 Baras et al.
2010/0157064 A1 6/2010 Cheng et al.
2010/0163612 A1 7/2010 Caillon
2010/0166303 A1 7/2010 Rahimi
2010/0174406 A1 7/2010 Miette et al.
2010/0286815 A1 11/2010 Zimmermann
2010/0289627 A1 * 11/2010 McAllister H04L 9/3226 340/10.42
2011/0026831 A1 2/2011 Perronnin et al.
2011/0064279 A1 3/2011 Uno
2011/0081043 A1 4/2011 Sabol et al.
2011/0091068 A1 4/2011 Stuck et al.
2011/0161117 A1 6/2011 Busque et al.
2011/0188709 A1 8/2011 Gupta et al.
2011/0194780 A1 8/2011 Li et al.
2011/0235920 A1 9/2011 Iwamoto et al.
2011/0267192 A1 11/2011 Goldman et al.
2012/0042171 A1 2/2012 White et al.
2012/0089639 A1 4/2012 Wang
2012/0130868 A1 5/2012 Loeken
2012/0177281 A1 7/2012 Frew
2012/0185393 A1 7/2012 Atsmon et al.
2012/0199651 A1 8/2012 Glazer
2012/0242481 A1 9/2012 Gernandt et al.
2012/0243797 A1 9/2012 Di Venuto Dayer et al.
2012/0250945 A1 10/2012 Peng et al.
2013/0110719 A1 5/2013 Carter et al.
2013/0162394 A1 6/2013 Etchegoyen
2013/0212027 A1 8/2013 Sharma et al.
2013/0214164 A1 8/2013 Zhang et al.
2013/0256415 A1 * 10/2013 Callegari B42D 15/0073 235/494
2013/0273968 A1 10/2013 Rhoads et al.
2013/0277425 A1 10/2013 Sharma et al.
2013/0284803 A1 10/2013 Wood et al.
2014/0032322 A1 1/2014 Schwieger et al.
2014/0140570 A1 5/2014 Ross et al.
2014/0140571 A1 5/2014 Elmenhurst et al.
2014/0184843 A1 7/2014 Campbell et al.
2014/0201094 A1 7/2014 Herrington et al.
2014/0270341 A1 9/2014 Elmenhurst et al.
2014/0314283 A1 10/2014 Harding
2014/0380446 A1 12/2014 Niu et al.
2015/0058142 A1 2/2015 Lenahan et al.
2015/0067346 A1 3/2015 Ross et al.
2015/0078629 A1 3/2015 Gottemukkula et al.
2015/0086068 A1 3/2015 Mulhearn et al.
2015/0110364 A1 4/2015 Niinuma et al.
2015/0117701 A1 4/2015 Ross et al.
2015/0127430 A1 5/2015 Hammer
2015/0248587 A1 9/2015 Oami et al.
2015/0294189 A1 10/2015 Benhimane et al.
2015/0309502 A1 * 10/2015 Breitgand G06Q 30/0185 700/98
2015/0371087 A1 12/2015 Ross et al.
2016/0034913 A1 2/2016 Zavarehi et al.
2016/0034914 A1 2/2016 Gonen et al.
2016/0055651 A1 2/2016 Oami
2016/0057138 A1 2/2016 Hoyos et al.
2016/0072626 A1 3/2016 Kouladjie
2016/0117631 A1 4/2016 McCloskey et al.
2016/0162734 A1 6/2016 Ross et al.
2016/0180485 A1 6/2016 Avila et al.
2016/0180546 A1 6/2016 Kim et al.
2016/0189510 A1 6/2016 Hutz

(56) **References Cited**

U.S. PATENT DOCUMENTS

2016/0203387	A1	7/2016	Lee et al.
2016/0300234	A1	10/2016	Moss-Pultz et al.
2016/0335520	A1	11/2016	Ross et al.
2017/0004444	A1	1/2017	Krasko et al.
2017/0032285	A1	2/2017	Sharma et al.
2017/0076132	A1	3/2017	Sezan et al.
2017/0132458	A1	5/2017	Short et al.
2017/0153069	A1	6/2017	Huang et al.
2017/0243230	A1	8/2017	Ross et al.
2017/0243231	A1	8/2017	Withrow et al.
2017/0243232	A1	8/2017	Ross et al.
2017/0243233	A1	8/2017	Land et al.
2017/0249491	A1	8/2017	Macintosh et al.
2017/0251143	A1	8/2017	Peruch et al.
2017/0253069	A1	9/2017	Kerkar et al.
2017/0295301	A1	10/2017	Liu et al.
2017/0300905	A1	10/2017	Withrow et al.
2017/0344823	A1	11/2017	Withrow et al.
2017/0344824	A1	11/2017	Martin
2017/0372327	A1	12/2017	Withrow
2018/0000359	A1	1/2018	Watanabe
2018/0012008	A1	1/2018	Withrow et al.
2018/0018627	A1	1/2018	Ross et al.
2018/0018838	A1	1/2018	Fankhauser et al.
2018/0024074	A1	1/2018	Ranieri et al.
2018/0024178	A1	1/2018	House et al.
2018/0047128	A1	2/2018	Ross et al.
2018/0053312	A1	2/2018	Ross et al.
2018/0121643	A1	5/2018	Talwerdi et al.
2018/0144211	A1	5/2018	Ross et al.
2018/0315058	A1	11/2018	Withrow et al.
2018/0349694	A1	12/2018	Ross et al.
2019/0026581	A1	1/2019	Leizerson
2019/0034518	A1	1/2019	Liu et al.
2019/0034694	A1	1/2019	Ross
2019/0102873	A1	4/2019	Wang et al.
2019/0102973	A1	4/2019	Oyama et al.
2019/0130082	A1	5/2019	Alameh et al.
2019/0228174	A1	7/2019	Withrow et al.
2019/0266373	A1	8/2019	Hirokawa
2019/0279017	A1	9/2019	Graham et al.
2019/0287118	A1	9/2019	Ross et al.
2019/0342102	A1	11/2019	Hao et al.
2019/0362186	A1	11/2019	Irshad et al.
2020/0153822	A1	5/2020	Land et al.
2020/0226366	A1	7/2020	Withrow et al.
2020/0233901	A1	7/2020	Crowley et al.
2020/0250395	A1	8/2020	Ross et al.
2020/0257791	A1	8/2020	Shannon et al.
2020/0334689	A1	10/2020	Withrow
2020/0349379	A1	11/2020	Ross
2020/0356772	A1	11/2020	Withrow et al.

FOREIGN PATENT DOCUMENTS

EP	0759596	A2	2/1997
EP	1016548	A2	7/2000
EP	1016549	A1	7/2000
EP	1719070	B1	4/2009
EP	2107506	A1	10/2009
EP	2166493	A1	3/2010
EP	2195621	B1	11/2013
EP	2866193	A1	4/2015
EP	2257909	B1	5/2015
EP	2869240	A2	5/2015
EP	2869241	A2	5/2015
EP	3208744	A1	8/2017
EP	3249581	A1	11/2017
EP	3267384	A1	1/2018
EP	3270342	A1	1/2018
EP	3435287	A2	1/2019
EP	3514715	A1	7/2019
GB	2097979	A	11/1982
GB	2482127	A	1/2012
JP	61234481	A	10/1986
JP	H07192112		7/1995
JP	2007213148	A	8/2007
JP	2010146158	A	7/2010
KR	20120009654	A	2/2012
WO	2005086616	A2	9/2005
WO	2006038114	A1	4/2006
WO	2007028799	A1	3/2007
WO	2007031176	A1	3/2007
WO	2007071788	A1	6/2007
WO	2007090437	A1	8/2007
WO	2007144598	A1	12/2007
WO	2009030853	A1	3/2009
WO	2009089126	A1	7/2009
WO	2009115611	A2	9/2009
WO	2010018464	A2	2/2010
WO	2010018646	A1	2/2010
WO	2012145842	A1	11/2012
WO	2013051019	A1	4/2013
WO	2013126221	A1	8/2013
WO	2013173408	A1	11/2013
WO	2015004434	A1	1/2015
WO	2016081831	A1	5/2016

OTHER PUBLICATIONS

Anonymous, "Intrinsic Characteristics for Authentication" & "Alp Vision Advances Security Through Digital Technology," Authentication News vol. 12, (No. 9) pp. 2, 7 and 8, dated Sep. 2006, 3 pages total.

Beekhof et al., "Secure Surface Identification Codes," Proceeding of the SPIE 6819: Security Forensics, Steganography, and Watermarking of Multimedia Contents X:68190D, 2008. (12 pages).

Boa et al., "Local Feature based Multiple Object Instance Identification using Scale and Rotation Invariant Implicit Shape Model," 12th Asian Conference on Computer Vision, Singapore, Singapore, Nov. 1-5, 2014, pp. 600-614.

Buchanan et al., "Fingerprinting documents and packaging," Nature 436 (7050): 475, 2005.

Cavoukian et al.; "Biometric Encryption: Technology for Strong Authentication Security and Privacy, Office of the Info. and Privacy Commissioner, Toronto, Ontario, CA," 2008, in WE, International Federation Iot Information Processing, Vo. 261; pp. 57-77.

Di Paola et al., "An Autonomous Mobile Robotic System for Surveillance of Indoor Environments," International Journal of Advanced Robotic Systems 7(1): 19-26, 2010.

Drew, M. S., et al., "Sharpening from Shadows: Sensor Transforms for Removing Shadows using a Single Image," Color and Imaging Conference, vol. 5, Society for Imaging Science and Technology, 2009, pp. 267-271.

Ebay, "eBay Launches Must-Have iPhone App RedLaser 3.0" https:/www.ebayinc.com/stories/news/ebay-launches-musthave-iphon-app-redlaser30/, Nov. 18, 2011 (Year: 2011), 8 pages.

Entropy.com Website History, Wayback Machine; https://web.archive.org/web/20 I 60330060808/https://www.entrupy.com/; Mar. 30, 2016 (Year: 2016), 2 pages.

Farid, "Digital Image Forensics", Dartmouth CS 89/189, Sprint 2013; 199 pages.

Fischler et al., "Random Sample Consensus: A Paradigm for Model Fitting with Applications to Image Analysis and Automated Cartography," Communication of the ACM 24(6); 381-395, 1981.

Huang et al., "A Novel Binarization Algorithm for Ballistic Imaging Systems," 3rd International Congress on Image and Signal Processing, Yantai, China, Oct. 16-18, 2010, pp. 1287-1291.

Huang, et al., "An Online Ballistics Imaging System for Firearm Identification"; 2nd International Conference on Signal Processing Systems, Dalian, China, Jul. 5-7, 2010, vol. 2, pp. 68-72.

Kartik et al., "Security System with Face Recognition, SMS Alert and Embedded Network Video Monitoring Terminal," International Journal of Security, Privacy and Trust Management 2(5):9-19, 2013.

Li, "Image Processing for the Positive Identification of Forensic Ballistics Specimens," Proceedings of the 6th International Conference of Information Fusion, Cairns, Australia, Jul. 8-11, 2003, pp. 1494-1498.

(56) **References Cited**

OTHER PUBLICATIONS

Li, "Firearm Identification System Based on Ballistics Image Processing," Congress on Image and Signal Processing, School of Computer and Information Science, Faculty of Computing, Health and Science Edith Cowan University, Perth, Australia pp. 149-154.
Maddern et al., "Illumination Invariant Imaging: Applications in Robust Vision-based Localization, Mapping and Classification for Autonomous Vehicles," IEEE International Conference on Robotics and Automation, Hong Kong, May 31-Jun. 7, 2014, 8 pages.
Matsumoto et al., "Nano-artifact metrics based on random collapse of resist," Scientific Reports 4:6142, 2014 (5 pages).
Mistry et al., "Comparison of Feature Detection and Matching Approaches: SIFT and SURF," Global Research and Development Journal for Engineering, vol. 2, Issue 4, Mar. 2017, 8 pages.
NCOA Link at http:/ /ribbs.usps.gov/ncoalink/ncoalink_print.htm; dated May 27, 2009; 3 pages.
Online NCOALink® Processing Acknowledgement Form (PAF) Released by Lorton Data, Jun. 2, 2009, URL=http://us.generation-nt.com/online-ncoalink-processing-acknowledgement-form-paf-released-by-press-1567191.html, download date Jun. 25, 2010, 1 page.
Rublee et al., "ORB: an efficient alternative to SIFT or SURF," IEEE International Conference on Computer Vision, Barcelona, Spain, Nov. 6-13, 2011, 8 pages.
Schneider et al., "A Robust Content Based Digital Signature for Image Authentication," Proceeding of the International Conference on Image Processing Lausanne, Switzerland, Sep. 19, 1996, pp. 227-230.
Schwabe Williamson & Wyatt, PC—Listing of Related Cases; dated Sep. 16, 2017; 2 pages.
Sharma et al., "The Fake vs Real Goods Problem: Microscopy and Machine Learning to the Rescue," KDD 2017 Applied Data Science Paper, Aug. 13-17, 2017, Halifax, NS, Canada, 9 pages.
Shi et al., "Smart Cameras: Fundamentals and Classification," Chapter 2, Belbachir (ed.), Smart Cameras, Springer, New York, New York, USA 2010, pp. 19-34.
Shields, "How To Shop Savvy With Red Laser," published online on Mar. 22, 2010; https ://i phone .appstomn .net/reviews/lifesty le/how-to-shop-savvy-with-redlaser /, downloaded Mar. 22, 2010, 8 pages).
Smith, "Fireball: A Forensic Ballistic Imaging System: Proceedings of the 31st Annual International Carnahan Conference on Security Technology," Canberra, Australia, Oct. 15-17, 1997, pp. 64-70.
Takahashi et al., "Mass-produced Parts Traceability System Based on Automated Scanning of Fingerprint of Things," 15th IAPR International Conference on Machine Vision Applications, Nagoya, Japan, May 8-12, 2017, 5 pages.
United States Postal Service Publication 28 "Postal Addressing Standards", dated Jul. 2008; text plus Appendix A only; 55 pages.
United States Postal Service, "NCOALink Systems", http:/ /www.usps.com/ncsc/addressservices/moveupdate/changeaddress.htm, website accessed Jun. 23, 2010, 2 pages.
Veena et al., "Automatic Theft Security System (Smart Surveillance Camera)," Computer Science & Information Technology 3:75-87, 2013.
Woods, "Counterfeit-spotting truth machine launches out of Dumbo," published online on Feb. 11, 2016, downloaded from http://technically/brooklyn/2016/02/11/entrupy-counterfeit-scanner/ on Mar. 20, 2019, 3 pages.
Farid, Ahmed , et al., "Integrated fingerprint verification method using a composite signature-based watermarking technique", Optical Engineering, The Catholic University of America, (Year: 2007), 6 pages.
Non-Final Office Action Issued in U.S. Appl. No. 16/866,468, dated Sep. 9, 2021, 24 pages.
European Search Report, dated Feb. 25, 2021, for European Application No. 20202130.9, 9 pages.
Extended European Search Report Application No. 21153877.2, dated Jun. 15, 2021, 8 pages.
Extended European Search Report, dated Aug. 18, 2021, for European Application No. 21164207.9—17 pages.
Extended European Search Report, dated Aug. 18, 2021, for European Application No. 21164207.9, 13 pages.
Extended European Search Report, dated Aug. 19, 2021, for European Application No. 21164353.1, 9 pages.
Extended European Search Report, dated Jun. 18, 2021, for European Application No. 21153355.9, 8 pages.
Non-Final Office Action Issued in U.S. Appl. No. 16/553,943, dated Sep. 1, 2021, 13 pages.
Non-Final Office Action Issued in U.S. Appl. No. 16/827,701, dated Aug. 17, 2021, 19 pages.
Non-Final Office Action Issued in U.S. Appl. No. 16/917,355, dated May 18, 2021, 26 pages.
Hensler, J., et al., "Hybrid Face Recognition Based on Real-time Multi-camera Stereo-Matching", ICIAP: International Conference on Image Analysis and Processing, 17th International Conference, Naples, Italy, Sep. 9-13, 2013, 10 pages.
Jain, Anil K, et al., "Biometric Cryptosystems: Issues and Challenges", Proceedings of the IEEE, IEEE, New York, US, vol. 92, No. 6, Jun. 1, 2004, XP011112757, pp. 948-960.
Scott, Von Duhn, et al., "Three-View Surveillance Video Based Face Modeling For Recognition", Biometrics Symposium, 2007, IEEE, PI, Sep. 30, 2007, 6 pages XP031202430.
Truong, Hieu C, et al., "Royal Canadian Mint/Signoptic Technologies Coin DNA Technology", World Money Fair (WMF) Berlin Feb. 1-3, 2011, http://www.amisdeleuro.org/upload/1340734488.pptx, 22 pages.
Zaeri, Naser, "Minutiae-based Fingerprint Extraction and Recognition, 2020 (year 2010)", 47 pages.

* cited by examiner

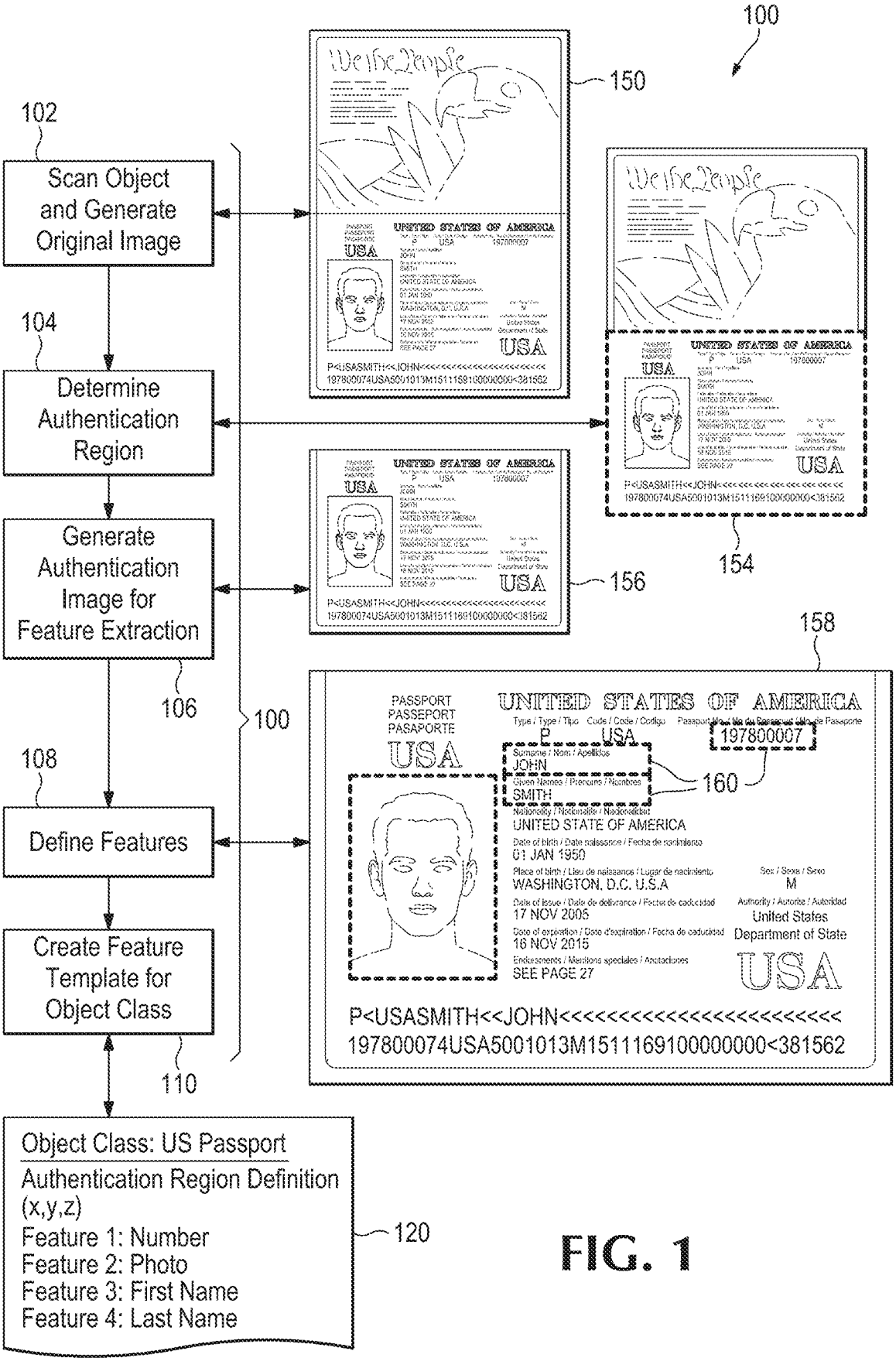

100
102
Scan Object and Generate Original Image
104
Determine Authentication Region
Generate Authentication Image for Feature Extraction
106
108
Define Features
Create Feature Template for Object Class
110
Object Class: US Passport
Authentication Region Definition (x,y,z)
Feature 1: Number
Feature 2: Photo
Feature 3: First Name
Feature 4: Last Name
120
150
154
156
158
160
UNITED STATES OF AMERICA
USA
JOHN
SMITH
UNITED STATE OF AMERICA
01 JAN 1950
WASHINGTON, D.C. U.S.A
M
17 NOV 2005
16 NOV 2015
United States Department of State
SEE PAGE 27
P<USASMITH<<JOHN<<<<<<<<<<<<<<<<<<<<<<<<
197800074USA5001013M1511169100000000<381562

FIG. 1

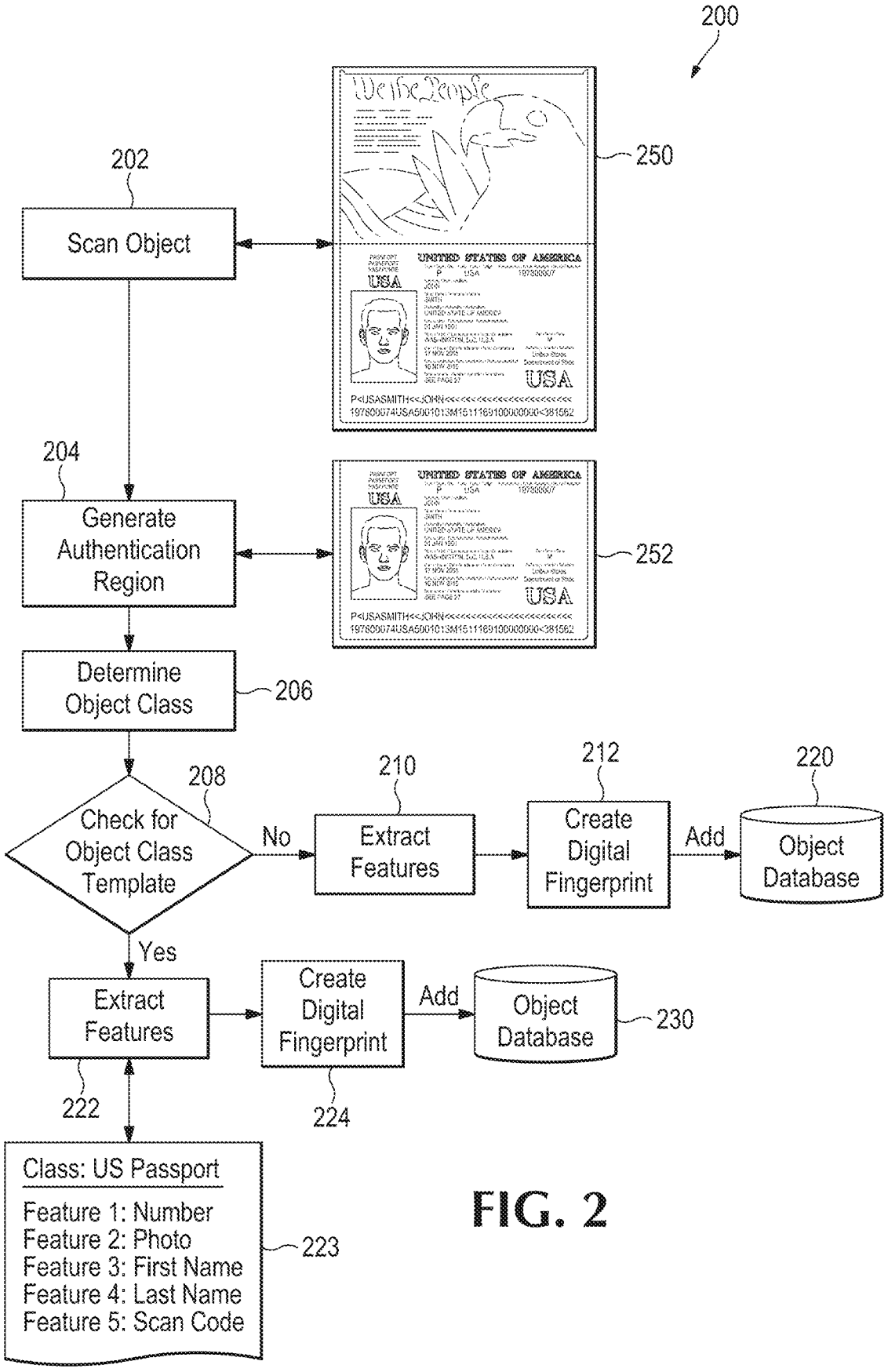

200
202
Scan Object
250
204
Generate Authentication Region
252
Determine Object Class
206
208
Check for Object Class Template
No
210
Extract Features
212
Create Digital Fingerprint
Add
220
Object Database
Yes
Extract Features
Create Digital Fingerprint
Add
Object Database
230
222
224
Class: US Passport
Feature 1: Number
Feature 2: Photo
Feature 3: First Name
Feature 4: Last Name
Feature 5: Scan Code
223

FIG. 2

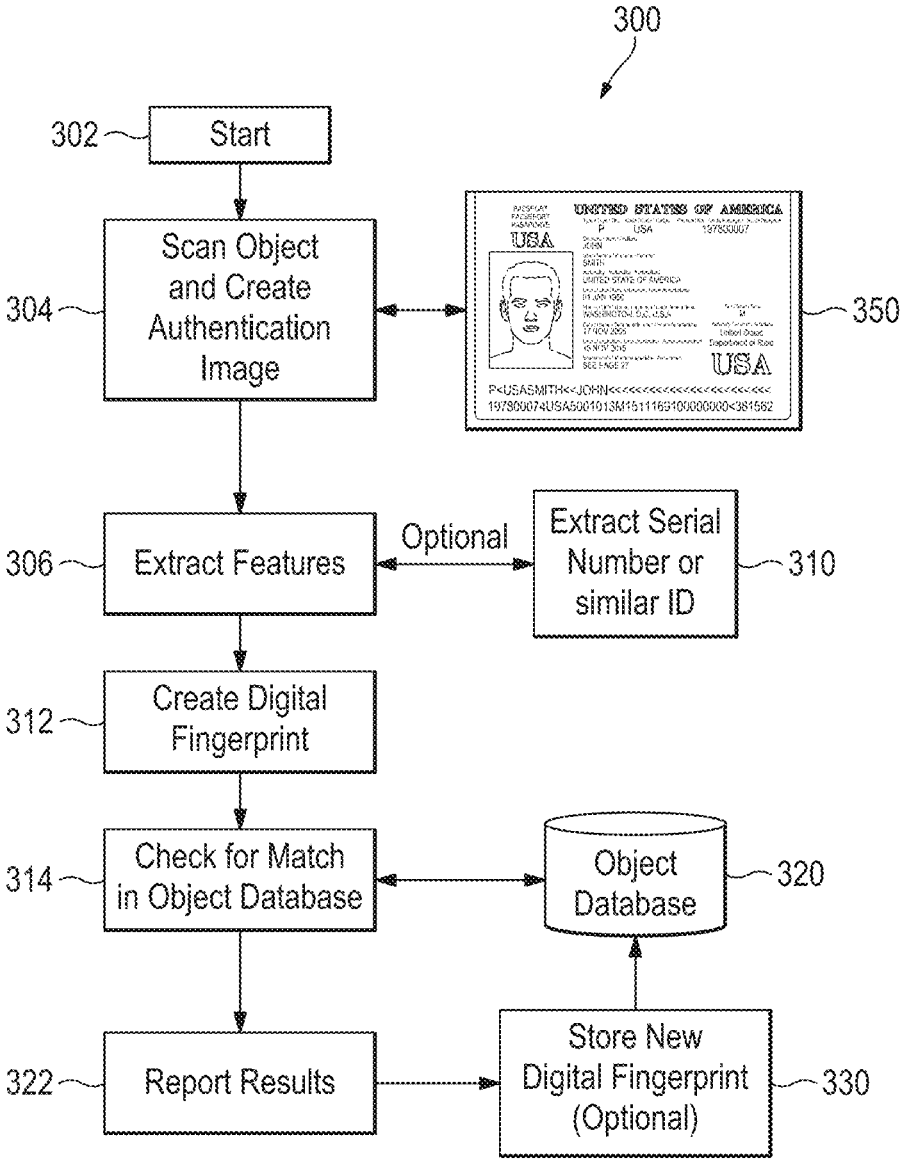

300
302
Start
Scan Object and Create Authentication Image
304
UNITED STATES OF AMERICA
USA
USA
P<USASMITH<<JOHN<<<<<<<<<<<<<<<<<<<<<<<<
350
Extract Features
306
Optional
Extract Serial Number or similar ID
310
Create Digital Fingerprint
312
Check for Match in Object Database
314
Object Database
320
Report Results
322
Store New Digital Fingerprint (Optional)
330

FIG. 3

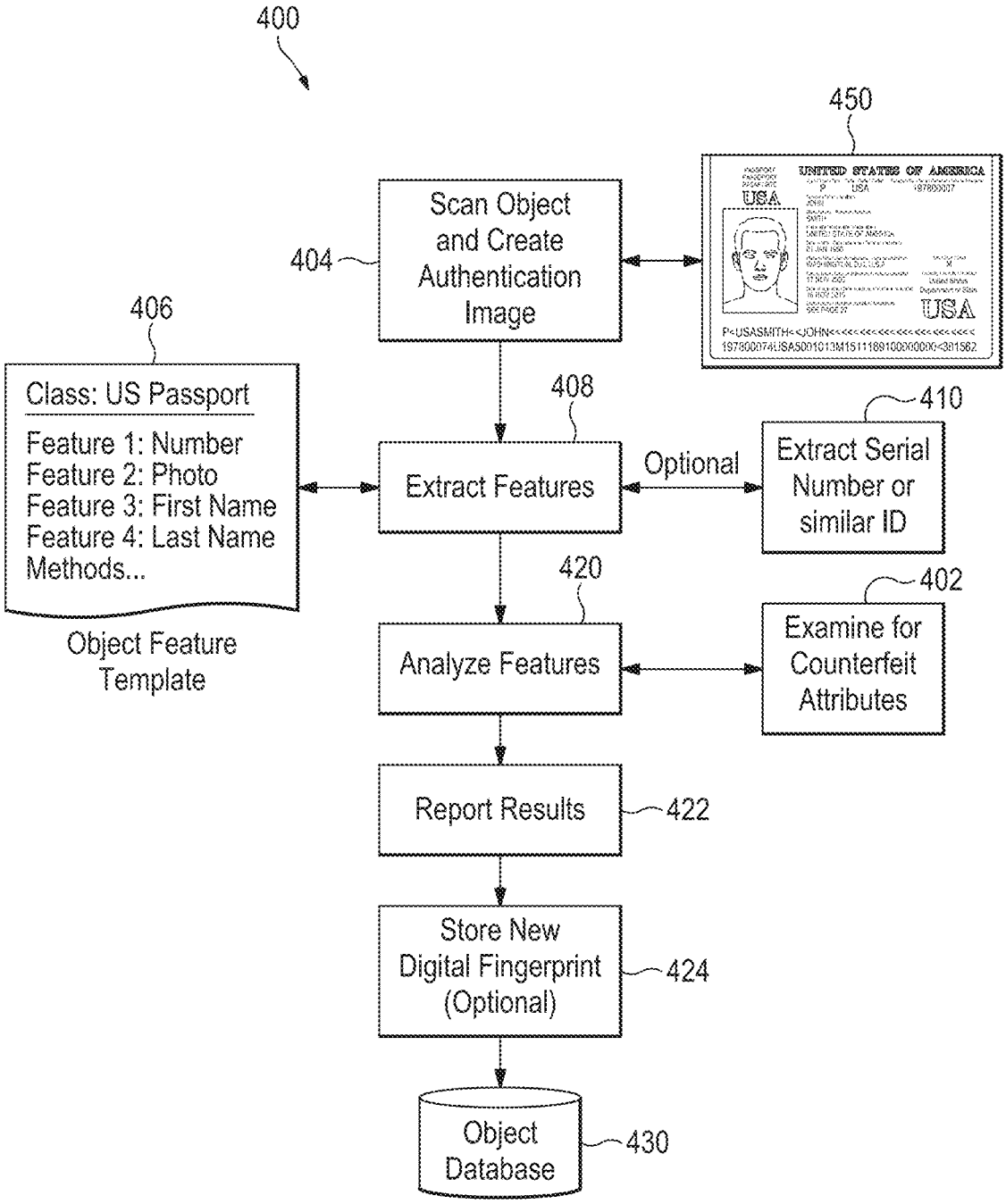

400
450
UNITED STATES OF AMERICA
USA
USA
P<USASMITH<<JOHN<<<<<<<<<<<<<<<<<<<<<<<<
404
Scan Object and Create Authentication Image
406
Class: US Passport
Feature 1: Number
Feature 2: Photo
Feature 3: First Name
Feature 4: Last Name
Methods...
Object Feature Template
408
Extract Features
Optional
410
Extract Serial Number or similar ID
420
Analyze Features
402
Examine for Counterfeit Attributes
Report Results
422
Store New Digital Fingerprint (Optional)
424
Object Database
430

FIG. 4

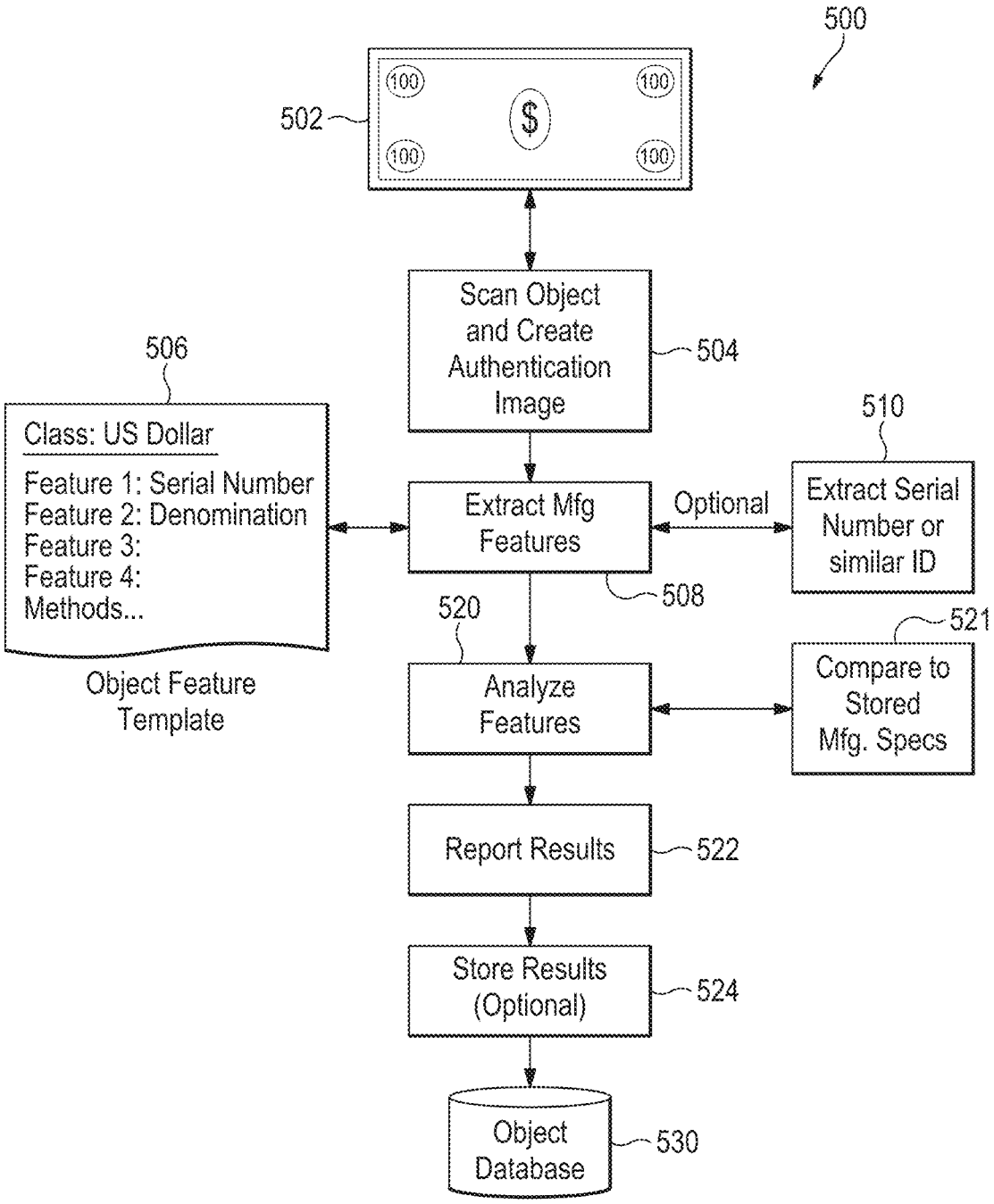

500
502
100
100
$
100
100
Scan Object and Create Authentication Image
504
506
Class: US Dollar
Feature 1: Serial Number
Feature 2: Denomination
Feature 3:
Feature 4:
Methods...
Object Feature Template
Extract Mfg Features
Optional
510
Extract Serial Number or similar ID
508
520
521
Analyze Features
Compare to Stored Mfg. Specs
Report Results
522
Store Results (Optional)
524
Object Database
530

FIG. 5

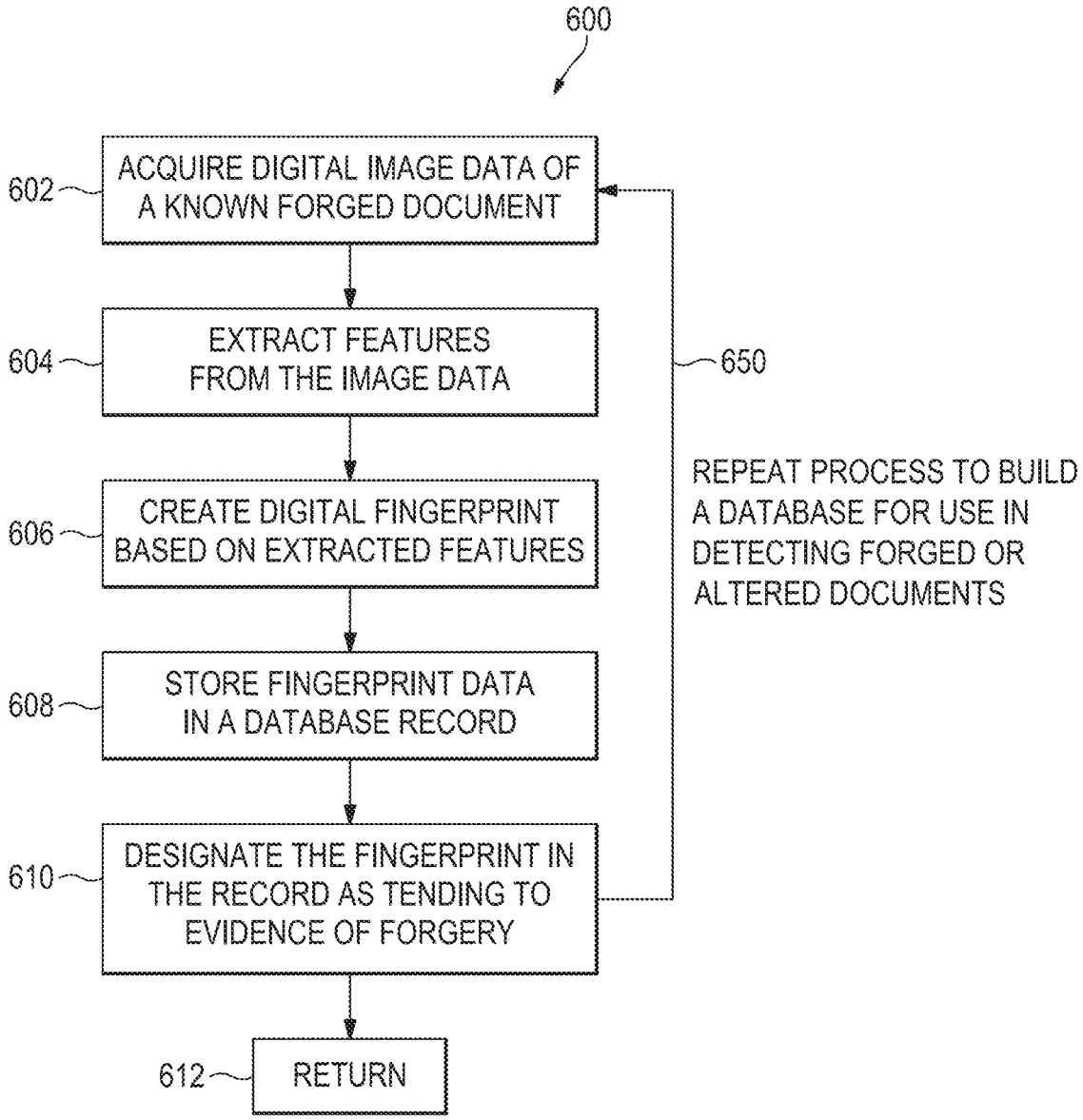
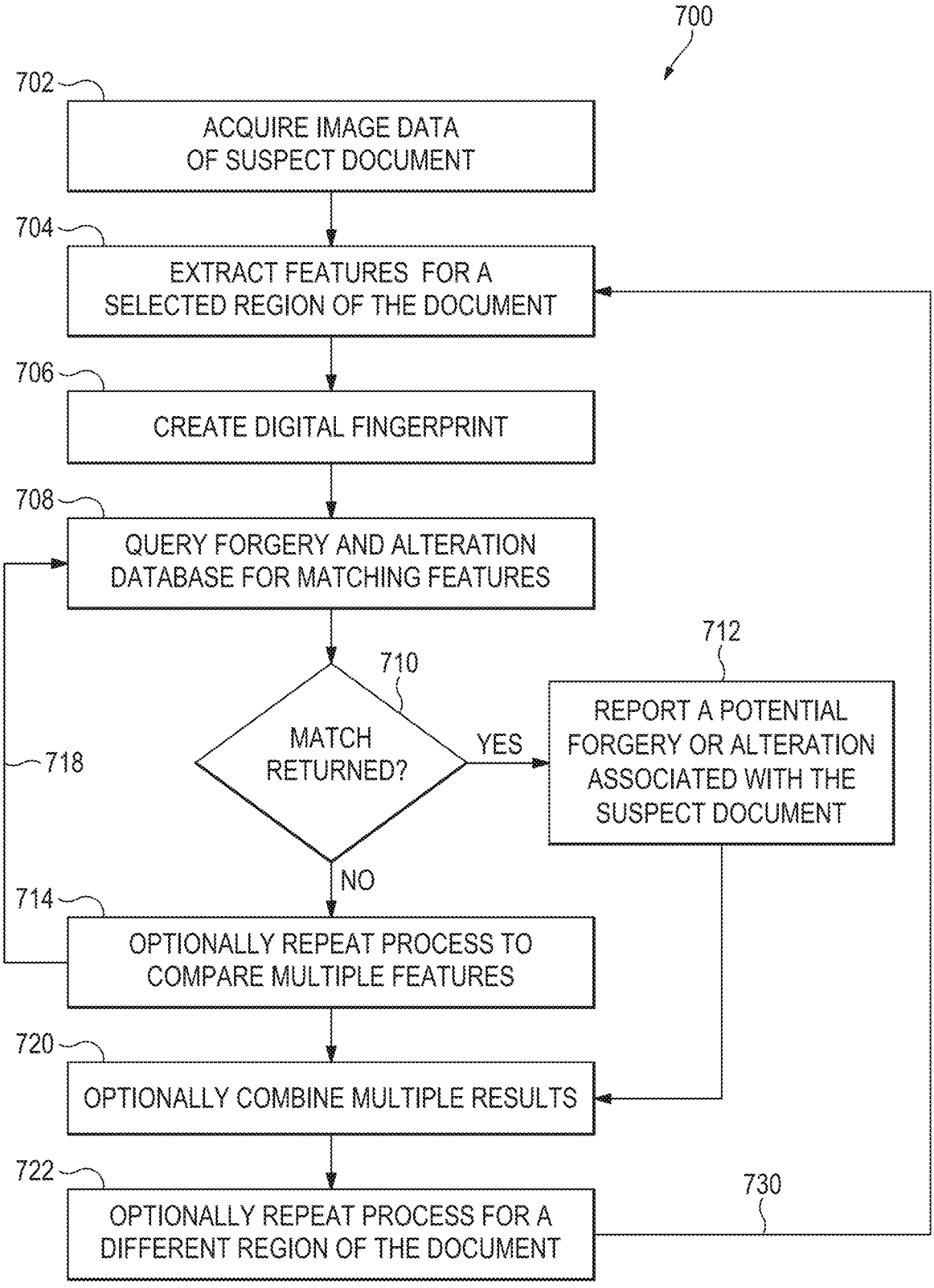

600
602
ACQUIRE DIGITAL IMAGE DATA OF A KNOWN FORGED DOCUMENT
604
EXTRACT FEATURES FROM THE IMAGE DATA
606
CREATE DIGITAL FINGERPRINT BASED ON EXTRACTED FEATURES
608
STORE FINGERPRINT DATA IN A DATABASE RECORD
610
DESIGNATE THE FINGERPRINT IN THE RECORD AS TENDING TO EVIDENCE OF FORGERY
612
RETURN
650
REPEAT PROCESS TO BUILD A DATABASE FOR USE IN DETECTING FORGED OR ALTERED DOCUMENTS
FORGERIES AND ALTERATIONS

FIG. 6



FORGERIES AND ALTERATION DETECTION

FIG. 7

FIG. 8

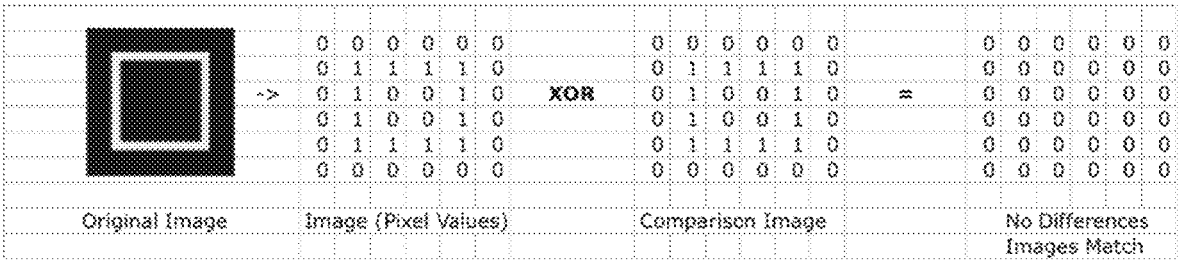

-> XOR =
Original Image
Image (Pixel Values)
Comparison Image
No Differences
Images Match

FIG. 9

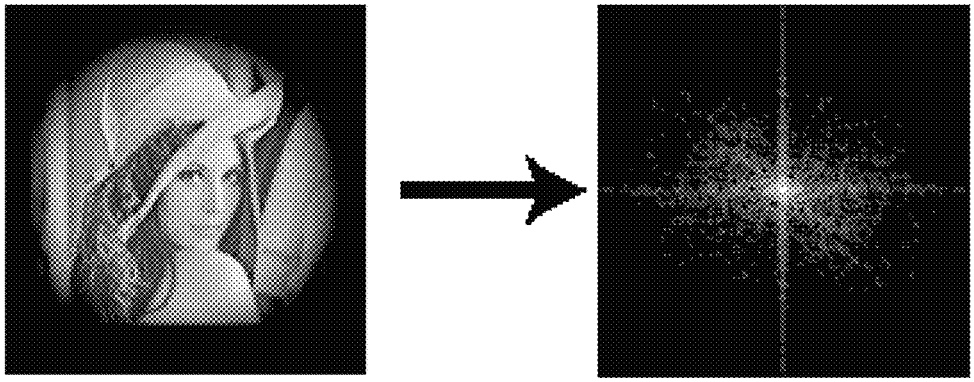


FIG. 10

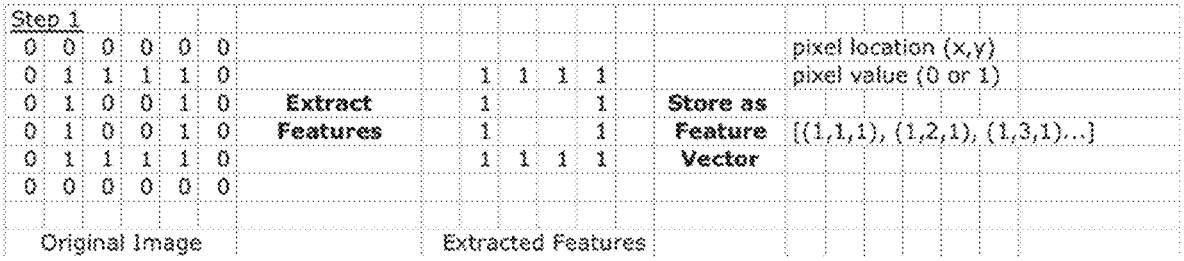


FIG. 11

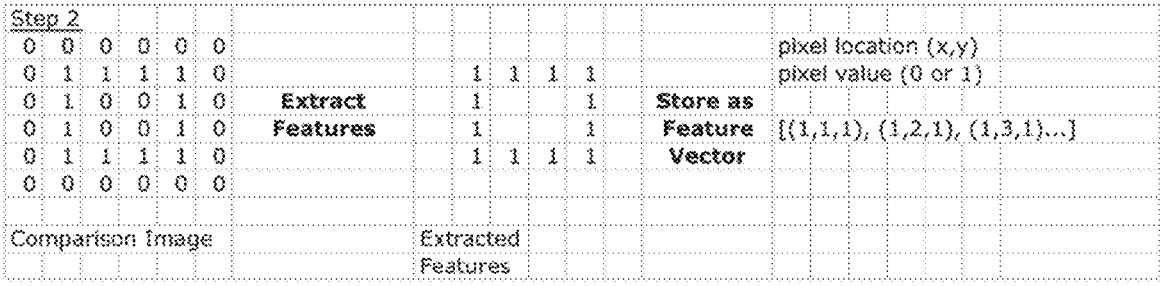


FIG. 12

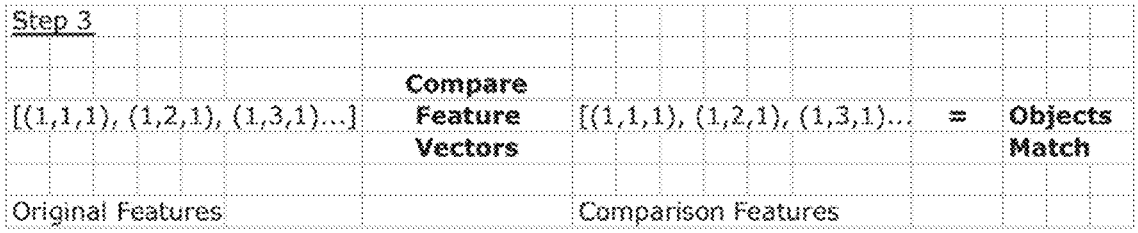


FIG. 13A

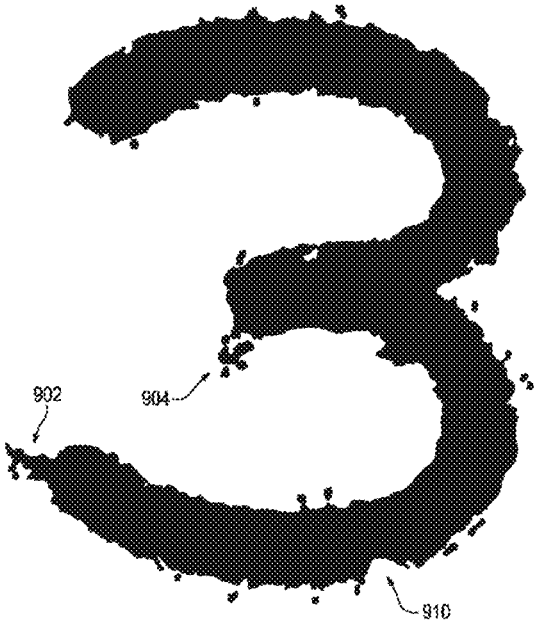


FIG. 13B

FIG. 14A

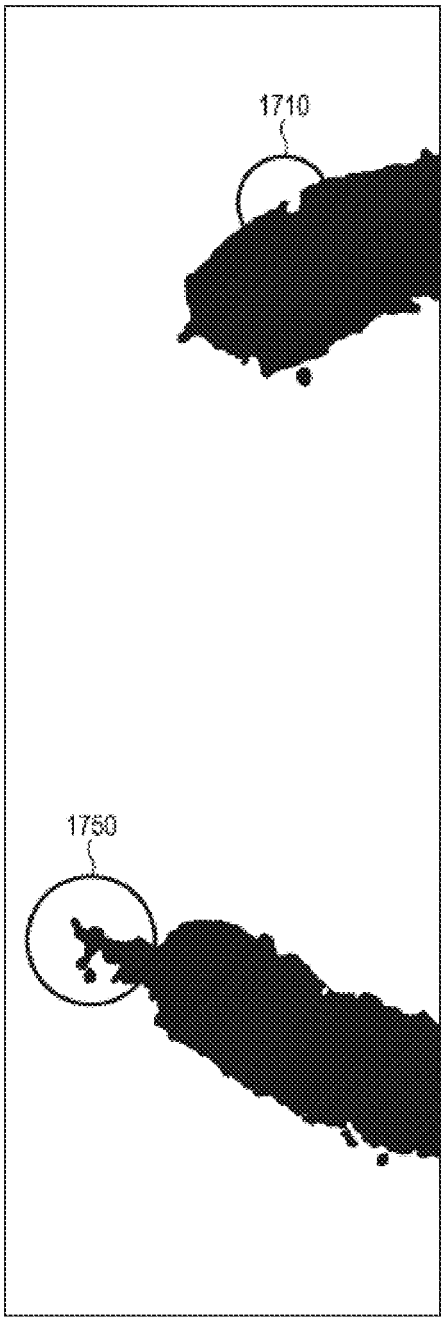


FIG. 14B

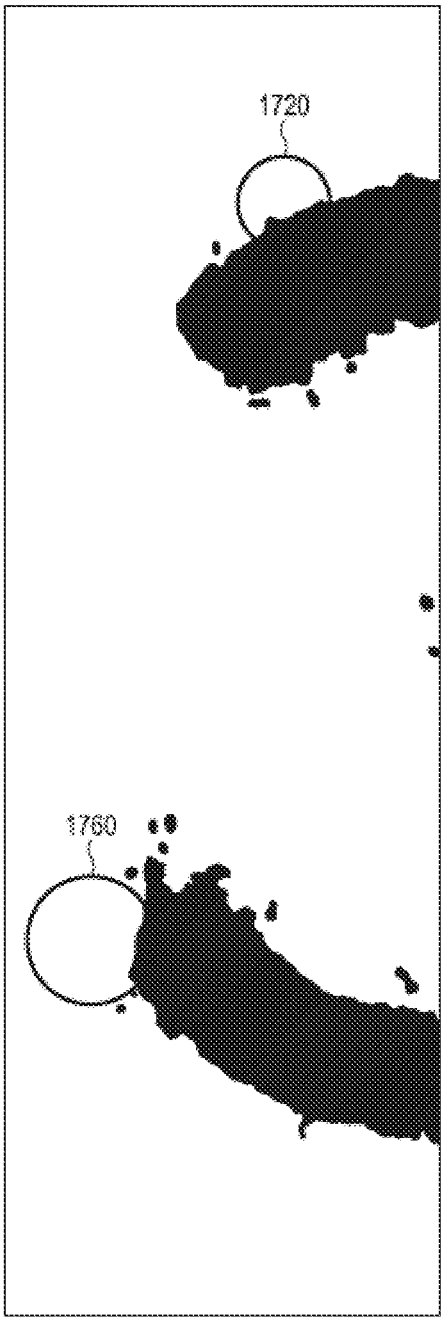


FIG. 15A

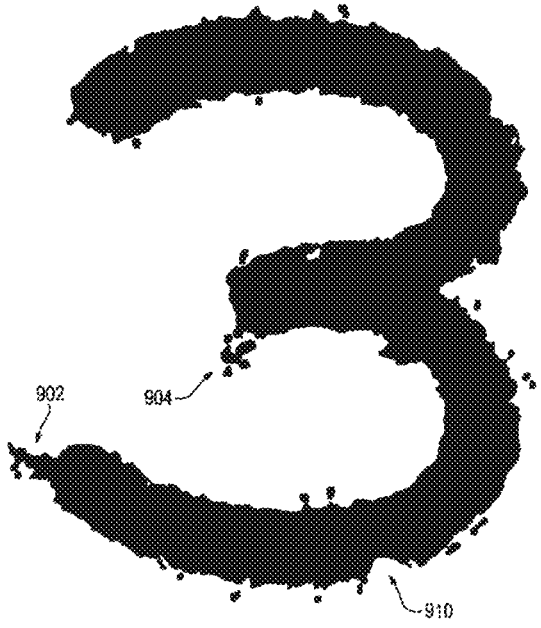


FIG. 15B

FIG. 16A

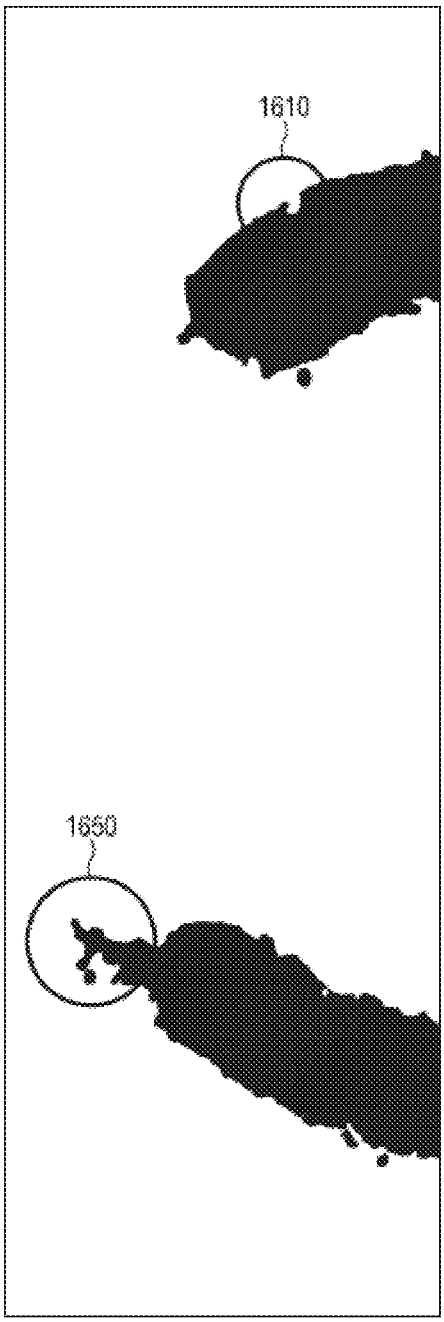


FIG. 16B

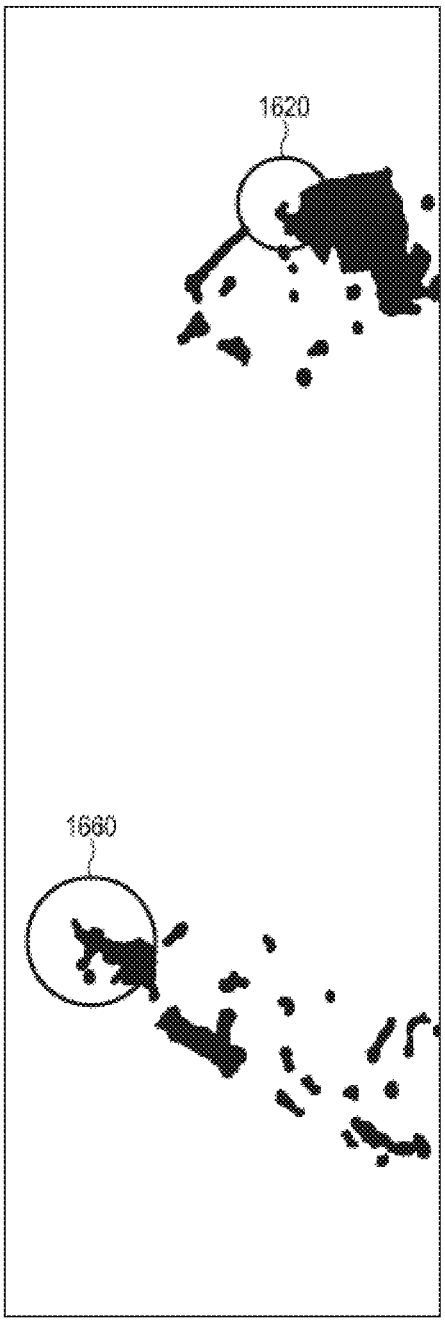
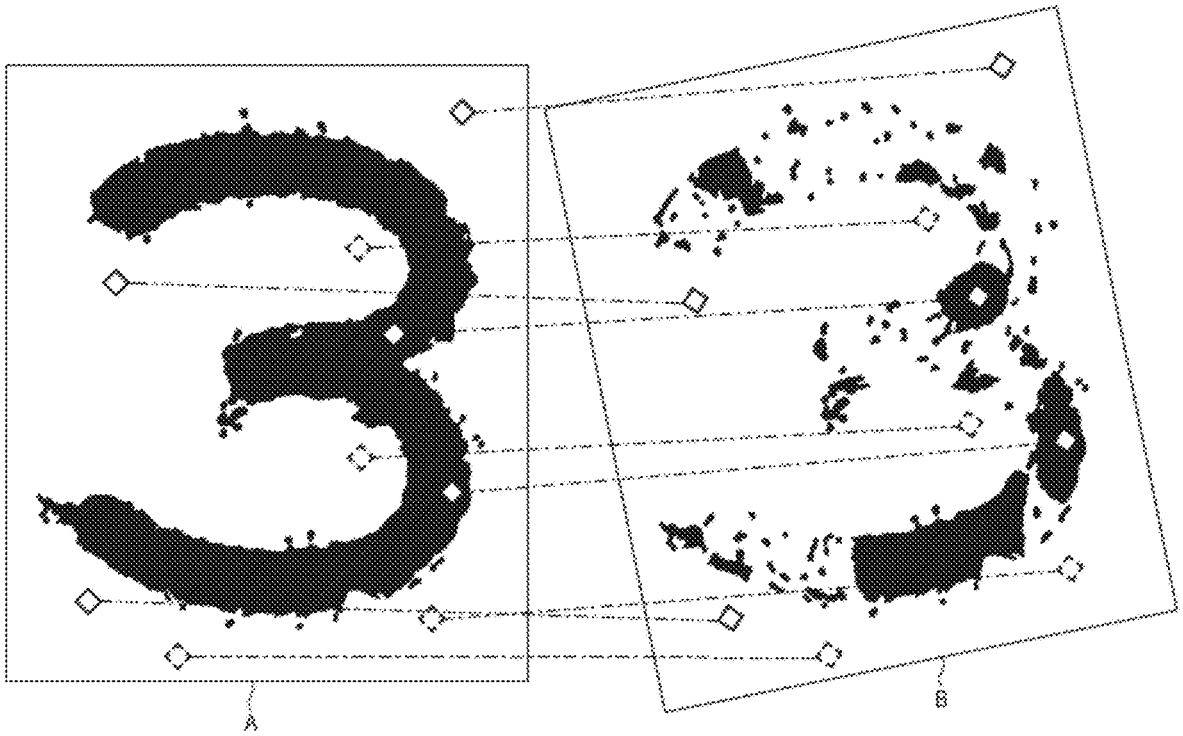


FIG. 17



DATABASE FOR DETECTING COUNTERFEIT ITEMS USING DIGITAL FINGERPRINT RECORDS

RELATED APPLICATIONS

This application is a continuation of U.S. application Ser. No. 15/862,556, filed Jan. 4, 2018, which is a continuation of U.S. application Ser. No. 15/208,328, filed Jul. 12, 2016 know U.S. Pat. No. 10,192,140), which is a divisional of U.S. application Ser. No. 14/531,724, filed Nov. 3, 2014 (now U.S. Pat. No. 9,443,298), which is a non-provisional, pursuant to 35 U.S.C. § 119(e), of U.S. provisional application No. 61/914,722 filed Dec. 11, 2013 and U.S. provisional application No. 61/898,780 filed Nov. 1, 2013, both incorporated herein by reference. application Ser. No. 14/531,724 is a continuation-in-part of U.S. application Ser. No. 14/290,653 filed May 29, 2014 (now U.S. Pat. No. 9,350,552) which is a continuation of U.S. application Ser. No. 13/410,753 filed Mar. 2, 2012 (now U.S. Pat. No. 8,774,455) which is a non-provisional, pursuant to 35 U.S.C. § 119(e), of U.S. provisional application No. 61/448,465 filed Mar. 2, 2011, each of which is incorporated herein by reference.

COPYRIGHT NOTICE

© 2018 Alitheon, Inc. A portion of the disclosure of this patent document contains material which is subject to copyright protection. The copyright owner has no objection to the facsimile reproduction by anyone of the patent document or the patent disclosure, as it appears in the Patent and Trademark Office patent file or records, but otherwise reserves all copyright rights whatsoever. 37 CFR § 1.71(d).

TECHNICAL FIELD

This invention pertains to methods and apparatus to identify and/or authenticate physical items, including documents, and more specifically to using a secure database of digital fingerprint records to detect a counterfeit item.

BACKGROUND OF THE INVENTION

Counterfeiting of manufactured goods is a worldwide problem, with recent studies estimating that 8% of the world's total GDP is now generated by the manufacturing and sales of counterfeit products. Many classes of counterfeit goods create substantial risks to public health including counterfeit pharmaceutical drugs, auto parts, pesticides, and children's toys. In addition, counterfeit computer chips, aerospace parts, and identification documents present significant risks to national security.

Many different approaches have been tried to uniquely identify and authenticate objects, including serial numbers, bar codes, holographic labels, RFID tags, and hidden patterns using security inks or special fibers. All of these methods can be duplicated, and many add a substantial extra cost to the production of the goods being protected. In addition, physically marking certain objects such as artwork, gemstones, and collector-grade coins can damage or destroy the value of the object.

If identifying or certifying information is stored separately from the object in the form of a label, tag, or certificate the entire identification/certification process must typically be performed again if the object is lost and later recovered, or its chain of control is otherwise compromised. There is a need for solutions that can prove the provenance of an object once the chain of custody is disrupted by the removal of the object from safe custody and/or the loss of the associated identification or certification information.

Other known techniques call for comparing bitmaps of images of the objects themselves, or selected regions of interest. Referring now to FIG. **8**, the image of the original object is taken and stored for reference. The whole image is stored, although it may be compressed for efficiency. When a new object is encountered, an image is taken of the new object and directly compared to the original image using XOR or similar algorithms. If there are no (or only statistically insignificant) differences, the images are declared a match and the object is authenticated. Further, FFT or similar transforms may be used to generate a "digital signature" of the image that can be used for comparison. See FIG. **9**. However, as in the previous case the same method is used—the resultant bitmapped image is compared with another bitmapped image, and if the pixels match the object is authenticated. Such methods are disclosed in U.S. Pat. No. 7,680,306 to Boutant et al. Bitmapped techniques are inefficient due to issues like file size, and have serious limitations that make them effectively unusable in most real world applications, due to variable lighting and orientation of the images, and the authentication of worn, damaged or otherwise altered objects.

SUMMARY OF THE INVENTION

The following is a summary of the invention in order to provide a basic understanding of some aspects of the invention. This summary is not intended to identify key/critical elements of the invention or to delineate the scope of the invention. Its sole purpose is to present some concepts of the invention in a simplified form as a prelude to the more detailed description that is presented later.

A physical object is scanned and a digital image of the object is created from the scan. A subset of the image known as an "authentication region" is selected. A set of features is extracted from the authentication region, which is sufficient to create a unique identifier or "digital fingerprint" for that object. The digital fingerprint may be registered in a database.

To select locations in an image to extract fingerprint features, a software process automatically selects a large number—typically hundreds or even thousands per square mm—of preferred areas of interest for purposes of digital fingerprint. A location may be of interest because of a relatively high level of content. That "content" in a preferred embodiment may comprise a gradient or vector, including a change in value and a direction.

In a preferred embodiment, each such area of interest is identified as a circle, for example, by centroid location and radius. Within each circular area of interest, the software then extracts one or more fingerprint features that define the relevant shapes within the corresponding circular location of the image. Each fingerprint feature preferably is stored as a feature vector as illustrated below. A feature vector preferably is an array of integer or floating point values describing an individual shape.

When an object is to be authenticated, a suitable system compares the digital fingerprint of the object to digital fingerprints previously stored in the database, and based on that comparison determines whether the object has been registered before, and is thus authentic. The digital fingerprint data specifies a set of features. Preferably, an "object feature template" may be created which has a list of specific

features and attributes that are relevant for authenticating a particular class of objects. A template may identify locations of particular features. One of the key advantages of the feature based method is that when the object is very worn from handling or use, the system can still identify the object as original, may be impossible with the bitmapped approach.

Another aspect of this disclosure relates to detecting a counterfeit or forged object, for example a document such as a drivers license or passport. In this case, there may be no "original" or source object digital fingerprint for comparison. Rather, "fingerprints" of known indicia of counterfeit or forged objects can be acquired and stored. For example, a large number of counterfeit New York State driver's licenses might be obtained by law enforcement officials in a raid or the like. Digital images of those forged documents can be acquired, and analyzed to form digital fingerprints, as described in more detail below. "Forgery feature vectors" of typical features that occur in the counterfeit licenses can be collected and stored in a database. Such indicia may include, for example, sharp, non-bleeding edges where a photograph has been replaced or torn paper fibers where an erasure occurred. These stored features from the counterfeit licenses can then be analyzed and stored as a reference set of fraudulent methods which can then be compared to new license fingerprints to detect a forged document. A count of "fraud indicator matches" can be compared to an empirical threshold to determine and quantify a confidence that a document is forged (or not).

Further, the fingerprinting approach described below can be used to determine whether a manufactured object meets its manufactured specifications. Applications of the system include but are not limited to object authentication, anti-counterfeiting, determining the provenance of an object, and compliance with manufacturing specifications.

Additional aspects and advantages of this invention will be apparent from the following detailed description of preferred embodiments, which proceeds with reference to the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is an example of an authentication region and object feature template definition for a U.S. passport.

FIG. **2** is a simplified flow diagram of a process for digital fingerprint generation and registration.

FIG. **3** is a simplified flow diagram of a process for authentication of a previously fingerprinted object.

FIG. **4** is a simplified flow diagram illustrating a process for object inspection to detect evidence of counterfeits.

FIG. **5** is a simplified flow diagram illustrating an object manufacturing inspection process.

FIG. **6** is a simplified flow diagram illustrating a method for building a database for use in detecting forged or altered documents.

FIG. **7** is a simplified flow diagram illustrating a method for using a digital fingerprint of a suspect document to detect a potential forger or alteration associated with the document.

FIG. **8** is a simplified diagram of a prior art bitmap comparison method for comparing images.

FIG. **9** is an example of a photograph and an image created by Fast Fourier Transform (FFT) of the image data.

FIG. **10** is a simple illustration of fingerprint feature extraction from an original digital image.

FIG. **11** is a simple illustration of fingerprint feature extraction from a comparison or candidate image.

FIG. **12** is a simple illustration of fingerprint feature comparison for identifying or authenticating an object.

FIG. **13**A shows an image of the numeral "3" representing the first digit in a serial number of an "original" or known U.S. dollar bill.

FIG. **13**B shows an image of the numeral "3" representing the first digit in a serial number a U.S. dollar bill to be authenticated.

FIG. **14**A is an illustration of results of reature extraction showing selected areas of interest in the image of FIG. **13**A.

FIG. **14**B is an illustration of results of feature extraction sowing selected areas of interest in the image of FIG. **13**B.

FIG. **15**A shows the same dollar bill image as in FIG. **13**A, juxtaposed with FIG. **15**B for comparison.

FIG. **15**B shows an image of the numeral "3" that has been damaged or degraded.

FIG. **16**A shows detail of two fingerprint feature locations on the numeral **3**.

FIG. **16**B shows detail of the damaged bill with the corresponding fingerprint feature locations called out for comparison.

FIG. **17** is a simplified illustration of a rotational transformation in the process of comparing digital fingerprints of two images.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

The methods described in this disclosure enable the identification of objects without attaching or associating any physical tags or materials with the object. A system does this by creating a unique digital signature for the object, which is referred to as a digital fingerprint. Digital fingerprinting utilizes the natural structure of the object, or essentially random features created incidental to the manufacturing process, to generate a unique digital signature for that object, much like a human fingerprint. Also like a human fingerprint, the digital fingerprint can be stored and retrieved to identify objects when they are encountered at a later date.

Eliminating the need to add tags or any physical modifications to the object offers a number of advantages to manufacturers, distributors, sellers and owners of goods. It reduces the cost of manufacturing, and is more secure than physical tagging. Physical tags may be lost, modified, stolen, duplicated, or counterfeited; digital fingerprints cannot.

Unlike prior art approaches that simply utilize a comparison of pixels, a system in accordance with this disclosure utilizes the extraction of features to identify and authenticate objects. Feature extraction enables us to take a large amount of information and reduce it to a smaller set of data points that can be processed more efficiently. For example, a large digital image that contains tens of thousands of pixels may be reduced to just a few features that can effectively identify the object. This reduced set of data we call a digital fingerprint. This digital fingerprint contains a set of individual fingerprint features which are stored as feature vectors. These vectors make image processing more efficient and reduce storage requirements, as the entire image need not be stored in the database, only the feature vectors. Examples of feature extraction algorithms include but are not limited to edge detection, corner detection, blob detection, wavelet features; Gabor, gradient and steerable output filter histograms, scale-invariant feature transformation, active contours, shape contexts and parameterized shapes.

While the most common applications of our system may be in the authentication of manufactured goods and documents, the system is designed to be applicable to any object that can be identified, characterized, quality tested, or authenticated with a digital fingerprint. These include but are

not limited to mail pieces, parcels, art, coins, currency, precious metals, gems, jewelry, apparel, mechanical parts, consumer goods, integrated circuits, firearms, pharmaceuticals and food and beverages. Here we use the term "system" in a broad sense, including our methods as well as apparatus arranged to implement such methods.

Scanning

In an embodiment, an object is scanned and identified either at initial manufacture or at the time of first contact with the system. This point of identification is preferably done when the item is either in the possession of its manufacturer, or has been transferred by secure means to the current holder so that its legitimacy at point of identification is adequately established. When such a process is impossible, as in the example of artworks or old coins, the object may be fingerprinted after the object is authenticated by an expert while its provenance is still secure.

In this application, we use the term "scan" in a broad sense. We refer to any means for capturing an image or set of images, which may be in digital form or transformed into digital form. The images may be two dimensional, three dimensional, or be in the form of a video. Thus a "scan" may refer to an image (or digital data that defines an image) captured by a scanner, a camera, a specially-adapted sensor array such as CCD array, a microscope, a smart phone camera, a video camera, an x-ray machine, etc. Broadly, any device that can sense and capture electromagnetic radiation that has traveled through an object, or reflected off of an object, is a candidate to create a "scan" of the object. Other means to extract "fingerprints" or features from an object may be used; for example, through sound, physical structure, chemical composition, or many others. The remainder of this application will use terms like "image" but when doing so, the broader uses of this technology should be implied. In other words, alternative means to extract "fingerprints" or features from an object should be considered equivalents within the scope of this disclosure.

Authentication Regions

Because the system works with many different types of objects, it is necessary to define what parts of the digital images of the objects are to be used for the extraction of features for authentication purposes. This can vary widely for different classes of objects. In some cases it is the image of the entire object; in other cases it will be a specific sub-region of the image of the object.

For instance, for a photograph we may want to use the digital image of the entire photograph for feature extraction. Each photograph is different, and there may be unique feature information anywhere in the photograph. So in this case, the authentication region will be the entire photograph.

Multiple regions may be used for fingerprints for several reasons, two of which are particularly important. It may be that there are several regions where significant variations take place among different similar objects that need to be distinguished while, in the same objects, there may be regions of little significance, i.e., in which there is little or no variation among different objects. In that case, the authentication region is used primarily to eliminate regions of little interest.

A bank note, for example, has a sufficient number of unique features that it can be authenticated if a few small arbitrary regions scattered across the surface are fingerprinted, along with recognizing the contents of a region telling the value of the bank note and one containing the bank note's serial number. In such a case the fingerprints of any region (along with sufficient additional information to determine the bank note's value and its purported identity) may be sufficient to establish the authenticity of the bill and multiple fingerprinted regions are used solely in the event that one or more regions may be absent (through, for example, tearing) when the bill is later presented for authentication.

Sometimes, however, specific regions of an item must be authenticated to ensure the item is both authentic and has not been altered. A passport provides an example. On a passport the features preferably used for authentication are extracted from regions containing such specific identification information as the passport number, recipient name, and recipient photo. In that case, we define a template of all those regions whose alteration from the original would invalidate the passport, such regions including the passport holder's photo and unique personal data.

FIG. **1** illustrates an example of an authentication region and object feature template definition for a U.S. passport. In this figure, brace **100** refers to a simplified flow diagram of a process as follows. At process block **102**, an object is scanned to generate an original "image"—technically a digital data file in any suitable format. We will simply refer to this data as an image. The original image is illustrated as the front page of a U.S. passport **150**. Next, the system processes the image data to determine an authentication region. For example, here the authentication region is the lower portion of image **150**, identified by dashed box **154**. Next the process generates an authentication image for feature extraction, block **106**. The image is illustrated at reference **156**. Next, at block **108**, the process defines one or more features for extraction. These are shown in the image **158** by dashed boxes **160**, for example, surname, given name, and passport number regions.

Finally, at block **110**, the process **100** comprises creating a feature template **120**. In this example, template **120** identifies an object class (U.S. Passport), defines an authentication regions (for example, by X-Y coordinates), and it lists one or more features within that authentication region. Here, the list comprises passport number, photo, first name and last name.

The ability to define and store the optimal authentication region for a given class of objects offers significant benefits to the user. In many cases it is much easier to scan a limited region of an object than the entire object. For instance, in the case of an article of designer clothing, it is much easier to take a picture of the manufacturer's label than it is to take a picture of the entire garment. Further, defining such regions enable the detection of partial alteration of the object.

Once an authentication region is defined, specific applications can be created for different markets and classes of objects that can assist the user in locating and scanning the optimal authentication region. For instance, an appropriately sized location box and crosshairs can automatically appear in the viewfinder of a smartphone camera application to help the user center the camera on the authentication region, and automatically lock onto the region and take the picture when the camera is focused on the correct area.

In many cases, objects may have permanent labels or other identifying information attached to them. These can also be used as features. For instance, wine may be put into a glass bottle and a label affixed to the bottle. Since it is possible for a label to be removed and reused, simply using the label itself as the authentication region is often not sufficient. In this case we may define the authentication region to include both the label and the substrate it is attached to—in this case some portion of the glass bottle. This "label and substrate" approach may be useful in defining authentication regions for many types of objects, such as

consumer goods and pharmaceutical packaging. If a label has been moved from it's original position, this can be an indication of tampering or counterfeiting. If the object has "tamper-proof" packaging, this may also be useful to include in the authentication region.

In some cases, we will want to use multiple authentication regions to extract unique features. For a firearm, for example, we might extract features from two different parts of the weapon. It is, of course, important that both match the original, but since the two parts may both have been taken from the original weapon and affixed to a weapon of substandard quality, it may also be important to determine whether their relative positions have changed as well. In other words it may be necessary to determine that the distance (or other characteristic) between Part A's authentication region and Part B's authentication region is effectively unchanged, and only if that is accomplished can the weapon be authenticated.

Object Feature Template Definition

When a new type or class of object is being scanned into the system for the first time, the system can create an Object Feature Template (as shown in FIG. **1**) that can be used to optimize subsequent authentication operations for that class of objects. This template can either be created automatically by the system, or by using a human-assisted process.

An Object Feature Template is not required for the system to authenticate an object, as the system can automatically extract features and create a digital fingerprint of an object without it. However, the presence of a template can greatly optimize the authentication process and add additional functionality to the system.

TABLE 1

Example Object Feature Template.

CLASS:
[Description of the object]
United States Passport
AUTHENTICATION REGION:
[Description of the authentication regions for the object]
Region 1: (x1, y1, z1), (x2, y2, z2)
.
.
Region n
REGION MATCH LIST
[List of the regions that are required to match to identify an object]
Region List: 1..n
FEATURES:
[Key features of the object]
Feature 1: Passport Number
Feature 2: Photo
Feature 3: First Name
Feature 4: Last Name
.
.
Feature n
METHODS:
[Programs that can be run on features of an object]
Feature 2:
Photo Method 1: [checkphoto.exe] Check for uneven edges indicating photo substitution
.
.
Method n

TABLE 1-continued

Example Object Feature Template.

Feature n
Method n
ADDITIONAL DATA
[Additional data associated with the object]
Data 1: example data
.
.
Data n

The uses of the Object Feature Template include but are not limited to determining the regions of interest on the object, the methods of extracting fingerprinting and other information from those regions of interest, and methods for comparing such features at different points in time. The name "object feature template" is not important; other data with similar functionality (but a different moniker) should be considered equivalent.

Four different but related uses for this technology are particularly in view in this disclosure. These are illustrative but are not intended to be limiting of the scope of the disclosure. These applications may be classified broadly as (1) authentication of a previously scanned original, (2) detection of alteration of a previously scanned original, (3) detection of a counterfeit object without benefit of an original, and (4) determination whether a manufactured item is within manufacturing or other applicable specification.

In case (1), the object is fingerprinted during the creation process (or while its provenance is unquestioned), or at the point where an expert has determined its authenticity and then the object is later re-fingerprinted, and the two sets of fingerprints are compared to establish authenticity of the object. This may be done by extracting a single fingerprint from the entire object or by extracting multiple sets of features from different authentication regions. It may also be facilitated by reading or otherwise detecting a serial number or other identifying characteristic of the object using optical character recognition or other means to make determining which original to compare it with easier. In many cases, manufacturing databases use serial numbers as identifiers. If we know the serial number we can directly access the database record for the object, and can directly compare the digital fingerprint to the original that was stored during the creation process, rather than searching the entire digital fingerprinting database for a match.

In case (2), the object is compared region by region with the original looking for low or nonexistent match of the fingerprint features from those regions. While case (1) is designed to determine whether the original object is now present, this case (2) is to determine whether the original object has been modified and if so, detecting how. In some embodiments, regions of interest having poor or no matching fingerprint features are presumed to have been altered.

In case (3), the item may not have been fingerprinted while its provenance was secure. An example would be legacy bills or passports created prior to initiating the use of a digital fingerprinting system during the creation process. In this case, the fingerprints of regions of interest may be compared with fingerprints from examples of known counterfeit objects, or with both those and fingerprints of known good objects. As an example, if a photo is added to a passport, the edge of the photo is liable to be sharper than the edge of the original, unaltered photo, indicating a cut and paste operation. Fingerprint characteristics of known good passports and those of passports known to have been altered

by changing the photograph can be compared with the passport being inspected to determine whether it shows features of alteration.

FIG. **6** is a simplified flow diagram of a process **600** for building a database for use in detecting counterfeit (forged or altered) objects. At process block **602**, digital image data is acquired of a known forged or altered document. Next, we extract features from the image data, as discussed above, block **604**. Continuing, at block **606** a digital fingerprint is created based on the extracted features.

The digital fingerprint data is stored in a database record, block **608**. Further, the record (digital fingerprint) is designated in the database as having features tending to evidence a forgery, block **610**. The basic process may be repeated, loop **650**, to acquire more images, and more features, to build the database.

Returning to case (4), the question of authenticity or alteration is not at issue. Instead we use the fingerprinting process to determine whether an object was manufactured sufficiently close to the manufacturing specification. In this case comparison of fingerprint features is against the ideal features of a presumed-perfect object, referred to as the "reference object". The reference object may exist (e.g. be one or more examples of the object that has been inspected by hand and declared good enough to serve as a standard) or may be a programmatic ideal. In this latter case the "ideal" fingerprint features will be generated manually or by a program rather than scanned off an original.

The Object Feature Template can contain a variety of information related to that class of objects. For instance, it would typically include the authentication region(s) for that class of objects, which authentication regions are required to determine a match, and a list of key features that are typically used in authenticating that object.

Additionally, a template can define methods to be applied to features that can be used to examine an object for signs of unauthorized modification or counterfeiting. For instance, every time a passport is scanned into the system, a program can automatically be run to examine the passport photo for signs of alteration. If the passport was fingerprinted at creation, fingerprints extracted from each such region at creation will be compared to fingerprints from corresponding regions when the passport is presented for authentication. If the passport was not fingerprinted at creation, the region template can be used, for example, to look for sharp, non-bleeding edges that can indicate where a photograph has been replaced or torn paper fibers can indicate where an erasure occurred. In addition to the examples discussed above, the Object Feature Template is designed to be extensible, and can store any additional data that is related to the object.

Digital Fingerprint Generation

Once an object has been scanned and at least one authentication region has been identified, the final digital image that will be used to create the unique digital fingerprint for the object is created. This image (or set of images) will provide the source information for the feature extraction process.

A "digital fingerprinting feature" is a feature of the object that is innate to the object itself, a result of the manufacturing process, a result of external processes, or of any other random or pseudo random process. For example, gemstones have a crystal pattern which provides an identifying feature set. Every gemstone is unique and every gem stone has a series of random flaws in its crystal structure. This crystal pattern may be used to generate feature vectors for identification and authentication.

A "feature" in this description is typically not concerned with reading or recognizing meaningful content by using methods like OCR (optical character recognition). For example, a label on a scanned object with a printed serial number may give rise to various features in fingerprint processing, some of which may become part of a digital fingerprint feature set or vector that is associated with the object. The features may refer to light and dark areas, locations, spacing, ink blobs, etc. This information may refer to the printed serial number on the label, but in the normal course of feature extraction during the fingerprinting process there is no effort to actually "read" or recognize the printed serial number.

As part of identifying the object, however, for ease of comparison of fingerprint features with those of the original which are stored in the object database, such information may in fact be read and stored by utilizing such techniques as optical character recognition. In many cases, serial numbers may be used as the primary index into a manufacturer's database, which may also contain the digital fingerprints. It would be far faster, for example, to determine whether a bank note being inspected is a match with a particular original if we can use the serial number, say "A93188871A" as an index into the digital fingerprinting database, rather than trying to determine which one it matches by iterating through many thousands of fingerprints. In this case (and in similar cases of weapon and passport serial numbers), the index recognition speeds up the comparison process but is not essential to it.

Once a suitable digital fingerprint of an object is generated, it may be stored or "registered" in a database. For example, in some embodiments, the digital fingerprint may comprise one or more fingerprint features which are stored as feature vectors. The database should be secure. In some embodiments, a unique ID such as a serial number also may be assigned to an object. An ID may be a convenient index in some applications. However, it is not essential, as a digital fingerprint itself can serve as a key for searching a database. In other words, by identifying an object by the unique features and characteristics of the object itself, arbitrary identifiers, labels, tags, etc. are unnecessary.

FIG. **2** is a simplified flow diagram of a process **200** for digital fingerprint generation and registration. In this case, the process begins with scanning the object, block **202**. An image **250** is acquired, in this illustration an U.S. passport is used. The next step is to identify or generate an authentication region, block **204**. For example, the authentication region may be the portion **252**. The authentication region may be identified, as discussed above, from an object feature template (see Table 1). Next an object class of the object is determined, block **206**. The result is used to check a database for a corresponding object class template, decision **208**. If there is no matching template, the process proceeds to extract features, block **210** without the aid of a template. A digital fingerprint is created based on the extracted feature, block **212**, and that digital fingerprint is stored in an object database **220**. Alternatively, if a matching object class template is found at decision **208**, the process continues to extract features, block **222**, utilizing the class template **223** to identify and locate the features. Then, a digital fingerprint is created from the resulting feature data, block **224**, and stored in a database **230**.

Authentication and Inspection Processes

When an object is presented, it is scanned and an image is generated. At that point, the steps to be followed depend on the operation to be performed. Several illustrative cases are discussed below.

Case #1: For authentication of a previously fingerprinted object, the following steps may be followed (see FIG. **3**, discussed below):

1. The authentication region (or regions) is either determined automatically by the system, or by utilizing the authentication region definitions stored in an Object Feature Template.
2. The relevant features are extracted from the authentication region(s) and the digital fingerprint is created. This will typically be in the form of feature vectors, but other data structures may be used as appropriate.
3. Optionally, a unique identifier such as a serial number may be extracted and stored to augment subsequent search and identification functions.
4. The digital fingerprint of the object to be authenticated is compared to the digital fingerprints stored in the database.
5. The system reports whether the object is authentic; i.e. whether it matches one of the digital fingerprints stored in the database.
6. The system may then store the digital fingerprint of the object to be authenticated in the database along with the results of the authentication process. Normally only the extracted features will be stored in the database, but the authentication image and/or the original image may be stored in the database for archival or audit purposes.

FIG. **3** illustrates such a process **300** in diagrammatic form. Beginning at start block **302**, the process scans an object and creates an authentication image, block **304**. The image is represented at **350**, again using the passport example. Features are extracted, block **306**, and optionally a serial number or similar ID number, preferably unique, may be extracted as well, block **310**.

The extracted data is processed to create a digital fingerprint, bloc **312**. An object database **320** may be queried for a matching fingerprint, block **314**. A "match" may be defined by a probability or similarity metric. Results of the database query may be reported to a user, block **322**. Finally, a new digital fingerprint may be stored into the database **320**, shown at process block **330**.

Case #2: For inspection of specific features of a previously fingerprinted object to determine whether they have been altered, the steps are similar to Case #1, but the process is used for the detection of alterations rather than authentication of the object:

1. The authentication region (or regions) is either determined automatically by the system, or by utilizing the authentication region definitions stored in an Object Feature Template.
2. The features to be inspected are extracted from the authentication region and the digital fingerprint is created. This will typically be in the form of feature vectors for the features to be inspected but other data structures may be used as appropriate.
3. Optionally, a unique identifier such as a serial number may be extracted and stored to be used to augment subsequent search and identification functions.
4. The digital fingerprint of the features to be inspected for alteration is compared to the fingerprint of the corresponding features from the original object stored in the database.
5. The system reports whether the object has been altered; i.e. whether the digital fingerprint of the features to be inspected match those previously stored in the database from the original object.
6. The system may then store the digital fingerprint of the features to be inspected in the database along with the results of the inspection process. Normally only the features will be stored in the database, but the authentication image and/or the original image may be stored in the database for archival or audit purposes.

Case #3: For inspection of the specific features of an object that has not been previously fingerprinted to determine whether the features have been altered, the following steps may be followed, referring now to FIG. **4**.

The system scans the object, block **404**, and creates an authentication image **450** that includes at least one authentication region. The authentication region (or regions) may be determined automatically by the system, or by utilizing the authentication region definitions defined in a stored Object Feature Template **406** as noted earlier. Either way, the process next extracts features from the authentication region(s), block **408**, and a digital fingerprint is created. This will typically be in the form of feature vectors, but other data structures may be used as appropriate.

The features of the object are then analyzed, block **420**, and examined for attributes indicative of a counterfeit, block **402**. Methods may be applied to the features by running programs that are listed in the Object Feature Template that check features for signs of counterfeiting. Features can also be statistically compared to features of other objects of the same class that are stored in the database using Bayesian algorithms or other methods to find suspect variations that the standard methods may not catch. Optionally, a serial number or similar ID may be extracted, block **410**.

The system preferably reports whether the object shows signs of alteration or counterfeiting, block **422**. The system may then store the digital fingerprint of the object to be inspected, block **424**, in the database **430** along with the results of the inspection process. Normally only the extracted features will be stored in the database, but the authentication image and/or the original image may be stored in the database for archival or audit purposes.

Case #4: For inspection of an object to determine whether it was manufactured in conformance with the manufacturer's specification, the following steps are followed; referring now to FIG. **5**. The authentication region (or regions) for an object **502** is determined by utilizing the authentication region definitions stored in an Object Feature Template **506**. In this illustration, the object **502** is a U.S. $100 bill. Scanning and creation of an authentication image are indicated at process block **504**.

The manufacturing features are extracted from the regions of interest, block **508**, and the digital fingerprint is created (not shown). This will typically be in the form of feature vectors for the manufacturing features, but other data structures may be used as appropriate. Optionally, a unique identifier such as a serial number may be extracted, block **510**, and stored to be used to augment subsequent search and identification functions.

Next, the digital fingerprint of the manufacturing features of the object to be checked is are analyzed, block **520**, and compared to a fingerprint of the manufacturing features from a reference object (i.e., a perfect manufactured object) stored in the database, illustrated at block **521**. In other words, in some embodiments, a reference object may be "fingerprinted" and used as a proxy for manufacture specifications. In other cases, the digital fingerprint of the object, and more

specifically the extracted feature vectors, may be compared to reference feature vectors that are based on manufacture specifications. This type of comparison speaks to quality of the object, but may not indicate provenance.

The system reports, block **522**, whether the manufactured object meets specifications; i.e. whether the digital fingerprint of the manufacturing features sufficiently match those stored in the database from the reference object. The system may then store the digital fingerprint of the manufacturing features in the database **530**, process block **524**, along with the results of the manufacturing inspection process. Normally only the extracted manufacturing features will be stored in the database, but the manufacturing inspection image and/or the original image may be stored in the database for archival or audit purposes.

Because in all of the above cases we may be extracting features from images produced under variable lighting conditions, it is highly unlikely two different "reads" will produce the exact same digital fingerprint. In a preferred embodiment, the system is arranged to look up and match items in the database when there is a "near miss." For example, two feature vectors [0, 1, 5, 5, 6, 8] and [0, 1, 6, 5, 6, 8] are not identical but by applying an appropriate difference metric the system can determine that they are close enough to say that they are from the same item that has been seen before. One example is to calculate Euclidean distance between the two vectors in multi-dimensional space, and compare the result to a threshold value. This is similar to the analysis of human fingerprints. Each fingerprint taken is slightly different, but the identification of key features allows a statistical match with a high degree of certainty.

FIG. **7** is a simplified flow diagram illustrating a method **700** for using a digital fingerprint of a suspect document to detect a potential forgery or alteration associated with the document. First, image data is acquired of a suspect document, block **702**. Then the process extracts features from a selected region of the document, block **704**. The extracted features are used to form a digital fingerprint, block **706**. Next the digital fingerprint or the extracted features are used to form a query, and the query is used to access a forgery/alteration database in search of a matching record, block **708**. If a matching record is returned, decision block **710**, then the system may report a potential forgery or alteration associated with the suspect document, block **712**. Optionally, multiple results may be combined in reaching a conclusion, block **720**, where such are available.

Referring again to decision block **710**, if no match is returned (i.e. no record matches the query criteria within a selected tolerance or confidence), then the process optionally may be repeated, block **714**, for comparison to additional database records. In other words, the database search may be expanded, see loop **718**. Again, multiple query results may be combined. Further, the entire process, defined by loop **730**, may be repeated for inspecting and analyzing additional or different regions of the document, block **722**. As discussed earlier, multiple regions of interest may be defined. Terminal conditions, not shown, may be implemented.

FIG. **10** is an illustration of an example of feature extraction from a digital image. The original image data, on the left, is searched by any of various software processes to detect and locate a feature in the image. In this case, the only important shape in this image is a square, and it extracts that feature, as shown in the middle of the figure, with "1" pixel values. (Most real implementations will have greater than one-bit pixel values.) Then, the extracted fingerprint feature may be stored as a feature vector as illustrated on the right side of the figure. A feature vector is an n-dimensional vector of numerical values that represent the shape.

In this approach, we may store only the features, not the entire image. In fact, after feature extraction the original image can be discarded. This has obvious advantages in terms of reduced storage requirements. Typical algorithms used for extracting features include but are not limited to edge detection, corner detection, blob detection, wavelet features; Gabor, gradient and steerable output filter histograms, scale-invariant feature transformation, active contours, shape contexts and parameterized shapes.

Referring now to FIG. **11**, it illustrates essentially the same process for accessing a comparison or candidate image, extracting features from that image, and again storing each of them as a feature vector. Note that the example above is presented solely for the purpose of explanation, and actual implementations will vary. For instance, many shapes can be parameterized and stored even more efficiently. Instead of storing all the pixels along the boundaries, the square in FIG. **10** could actually just be stored as the lower left and upper right corner points ((x**1**, y**1**), (x**2**, y**2**)). Similarly, a circle could be stored with just the center point and radius. Feature vectors can store a wide variety of n-dimensional representations such as point, lines, polylines, edges, ridges, histograms and many others.

Once the features are extracted from the original image and the candidate image, the features can be compared directly to determine if there is a match. Typical algorithms for comparing features include but are not limited to nearest neighbor, hashing, indexing feature sets with visual vocabularies, support vector machines, multilayer perceptron and random forests and ferns. A comparison of these feature vectors is illustrated in FIG. **12**, resulting in a match.

FIG. **13**A illustrates an image of the numeral "3" representing a number printed on an "original" or known U.S. dollar bill. This bill may have been fingerprinted, for example, at the time of manufacture or public release, as described herein. As noted below, fingerprint databases of currency and the like may be secured. And such databases preferably exclude raw image data. This image, on the order of about 40× magnification, shows a couple of distinctive features visible to the naked eye.

FIG. **13**B illustrates an image of a number printed on a second or unknown U.S. dollar bill. This second bill may be fingerprinted using the same process, and then the resulting digital fingerprints, i.e., the respective fingerprint feature vectors, may be compared as further explained below, to determine whether or not the second bill is in fact the same one as the first bill, even though it may have changed from wear and tear.

FIG. **14**A is a simplified illustration of the results of feature extraction applied to the numeral **3** of FIG. **13**A. (Only the ends of the numeral are shown.) Two areas of interest are called out by circles **1720** and **1750**. Below we discuss how these areas may be selected in an image. Fingerprint feature extraction is applied to each of these circular regions. The results for each location are stored in fingerprint feature vectors. A collection of feature vectors, say for location **1750**, may be stored as a feature vector array. FIG. **14**B is a simplified illustration of the results of feature extraction applied to the numeral **3** of FIG. **13**B. The same fingerprinting process is applied to this image. The same locations of interest as in FIG. **14**A are labeled **1720** and **1760**, respectively. Then the stored features (from the original object) are compared with the features extracted

from the new object. As in this case, if the features are not encountered in the second object, it is not a match.

One of the key advantages to the feature-based method is that when the object is very worn from handling or use, the system can still identify the object as original, which may be impossible with the bitmapped approach. FIG. **15**A shows the same dollar bill image as in FIG. **13**A, juxtaposed with FIG. **15**B for comparison. FIG. **15**B shows the same bill after machine washing, perhaps in someone's pocket.

In FIG. **15**B, the image (actually the dollar bill) has been degraded; there is significant loss of ink and destruction of the paper surface in multiple locations. A bit mapped approach would clearly fail to match up here, as the number of pixels that are different is significant—only relatively few of the pixels are the same as the original.

FIG. **16**A shows the detail of two fingerprint feature locations as before, **1610** and **1650**. FIG. **16**B shows detail of the damaged bill with the corresponding locations called out as **1620** and **1660**, respectively. Here, one can see visually why a comparison of the corresponding fingerprint feature vectors would be adequate to result in a match. In practice, a much larger number of features would be used.

The image of the damaged bill is analyzed by a processor. The processor accesses a database of previously stored fingerprint data. If the dollar bill serial number is legible (by eye or machine), the record for the corresponding bill may be accessed from the datastore using the serial number as an index. Similarly, if any portion of the serial number is legible, the search for a matching record can be narrowed on that basis. Either way, a candidate record, containing a set of stored regions of interest may be compared to the suspect image.

As explained above, in addition to being able to recognize a worn object, the feature-based approach can deal with problems like rotated images. This is especially important in a system where the retail customer may be taking a picture of an object to be authenticated. In this case external factors like lighting and rotation are not under the manufacturer's control.

Referring now to FIG. **17**, it shows the original image on the left side, with a small set of fingerprint features marked as small diamond shapes. This is merely a callout symbol for illustration. In a preferred implementation, as noted, circular areas are used. For each feature (preferably identified in the database record), a search is conducted of the suspect image on the right side of FIG. **17** for a matching feature. The position may not match exactly, due to "stretch"—an effective difference in magnification, and/or due to rotation of the image. Although it may not match locations literally; a mathematical transformation can be defined that maps one image to the other, thereby accounting for rotation and stretch as appropriate. Thus, a bounding rectangle A indicated by the box in the left side image may be mapped to a quadrilateral indicated by the line B in the right side image.

Once an appropriate transformation is found, further matching can be done to increase the level of confidence of the match if desired. In some applications, a number of matches on the order of tens or hundreds of match points is sufficient. On the other hand, the number of non-match points also should be taken into account. That number should be relatively very low, but it may be non-zero due to random dirt, system "noise" and the like. Preferably, the allowed mapping or transformation should be restricted depending on the type of objects under inspection. For instance, some objects may be inflexible, which may restrict the possible deformations of the object.

To summarize the imaging requirements for a typical fingerprinting system, for example for inspecting documents, it should provide sufficient imaging capability to show invariant features. The particulars will depend on the regions used for authentication. For many applications, 10× magnification is adequate. For ink bleeds on passports, bills and other high-value authentication, 40× power is more than sufficient. In preferred embodiments, the software should implement a flexible response to accommodate misalignment (rotation), orientation and scale changes. Color imaging and analysis is generally not required for using the processes described above.

Hardware and Software

Most of the equipment discussed above comprises hardware and associated software. For example, the typical portable device is likely to include one or more processors and software executable on those processors to carry out the operations described. We use the term software herein in its commonly understood sense to refer to programs or routines (subroutines, objects, plug-ins, etc.), as well as data, usable by a machine or processor. As is well known, computer programs generally comprise instructions that are stored in machine-readable or computer-readable storage media. Some embodiments of the present invention may include executable programs or instructions that are stored in machine-readable or computer-readable storage media, such as a digital memory. We do not imply that a "computer" in the conventional sense is required in any particular embodiment. For example, various processors, embedded or otherwise, may be used in equipment such as the components described herein.

Memory for storing software again is well known. In some embodiments, memory associated with a given processor may be stored in the same physical device as the processor ("on-board" memory); for example, RAM or FLASH memory disposed within an integrated circuit microprocessor or the like. In other examples, the memory comprises an independent device, such as an external disk drive, storage array, or portable FLASH key fob. In such cases, the memory becomes "associated" with the digital processor when the two are operatively coupled together, or in communication with each other, for example by an I/O port, network connection, etc. such that the processor can read a file stored on the memory. Associated memory may be "read only" by design (ROM) or by virtue of permission settings, or not. Other examples include but are not limited to WORM, EPROM, EEPROM, FLASH, etc. Those technologies often are implemented in solid state semiconductor devices. Other memories may comprise moving parts, such as a conventional rotating disk drive. All such memories are "machine readable" or "computer-readable" and may be used to store executable instructions for implementing the functions described herein.

A "software product" refers to a memory device in which a series of executable instructions are stored in a machine-readable form so that a suitable machine or processor, with appropriate access to the software product, can execute the instructions to carry out a process implemented by the instructions. Software products are sometimes used to distribute software. Any type of machine-readable memory, including without limitation those summarized above, may be used to make a software product. That said, it is also known that software can be distributed via electronic transmission ("download"), in which case there typically will be

a corresponding software product at the transmitting end of the transmission, or the receiving end, or both.

Integration with Bill Processing Equipment

We propose creation of fingerprint data at the U.S. Treasury or any other producer (printer) of negotiable bills or notes. Preferably, such a system utilizes random, microscopic features unique to each bill's paper and printing. For example, the system may extract features from unpublished locations on the bills. In other words, the specific locations used for authentication are maintained in secrecy. The extracted features may be converted into encrypted feature vectors and associated in a data store with the corresponding bill serial number (the serial number having been readily captured by the same scanner or a separate one). In this way, a protected database may be created that is addressable or searchable by serial number or feature vector, but only by authorized users. (Here, a "user" may be a machine with electronic access to the database.)

Equipment is known for stacking, counting, and "strapping" paper money notes. A "strap" is a package of 100 notes, held together by a single paper band, as required for deposit by U.S. Federal Reserve rules. Various note handling equipment may be modified to include a digital scanner, for example, an optical scanner, to capture images of each bill or note as it is processed. The scanner may be coupled to a suitable processor, as explained above, for storing the captured images, and for processing the images to authenticate them and/or to detect counterfeit items.

Preferably, such a system is granted access to the protected database that is searchable by serial number or digital fingerprint. It may then look up each bill scanned, and compare features of the digital image to the digital fingerprint stored in protected database for the corresponding serial number. This process may be done by batch or in real time or near real time. The comparison, as further described above, may provide a confidence metric, or a simple yes/no (authentic/counterfeit) result for each note. It may identify a counterfeit note by serial number, but also by sequence number to facilitate locating the bill ("the 28^{th} bill in the strap #218"). In this way, a bank or other institution can detect counterfeit notes in a timely manner.

In another embodiment, a scanner, which may be portable and optionally wireless, may be made available at a bank teller station for the teller to authenticate bills presented for deposit or exchange. Further, such a system may be installed at an ATM machine to automatically authenticate bills presented for deposit. The ATM may be programmed to accept the bills to get them "off the street" but flag them as counterfeit or suspect.

The term "note" is commonly used in the U.K. with regard to paper money, while the term "bill" is more common in the U.S. We use them interchangeably here. Not to be confused with U.S. Treasury "bills" and "notes" which are not currency but debt instruments. That said, the inventions disclosed herein are applicable to those as well as currency, although nowadays such things are mainly processed by electronic "book entries" rather than paper documents. Older U.S. Savings Bonds, and any other bearer instruments in any country, can all be authenticated by various embodiments of the present invention.

Having described and illustrated the principles of the disclosure and some illustrative embodiments thereof, it should be apparent that the invention may be modified in arrangement and detail without departing from such principles. For convenience, we summarize below some aspects of the disclosure. The following list is merely illustrative and not intended to limit or define all the inventions disclosed. The scope of the present invention should, therefore, be determined only by the following claims.

The invention claimed is:

1. A machine comprising:

an input device that captures image data of at least a portion of a suspect physical object; and

a digital fingerprint system having a processor and a memory wherein the processor is configured to

create a digital fingerprint of the suspect physical object based on the image data, wherein the digital fingerprint includes a first piece of data identifying a plurality of regions of interest of the suspect physical object and, for each region of interest, a second piece of data forming at least one fingerprint feature vector that describes a fingerprint feature extracted from the region of interest of the suspect physical object;

store the created digital fingerprint for the suspect physical object in a database, the database having stored therein multiple digital fingerprints associated with multiple physical objects, wherein the digital fingerprint identifies the suspect physical object as being unique among the multiple physical objects.

2. The machine of claim **1**, wherein the input device includes at least one optical sensor.

3. The machine of claim **1**, wherein the fingerprint feature includes manufacturing features of the suspect physical object.

4. The machine of claim **1**, wherein the processor of the digital fingerprint system is further configured to extract a unique identifier from the suspect physical object; and

store the unique identifier in the database to augment search and identification of the suspect physical object.

5. The machine of claim **1**, wherein the input device further captures image data of at least a portion of a reference physical object that is manufactured according to a specification of a manufacturer; and

the processor of the digital fingerprint system is further configured to create a digital fingerprint of the reference physical object, wherein the digital fingerprint of the reference physical object includes a first piece of data identifying a plurality of regions of interest of the reference physical object and, for each region of interest, a second piece of data forming at least one reference feature vector that describes a fingerprint feature extracted from the region of interest of the reference physical object, wherein the digital fingerprint of the reference physical object serves as a proxy for the specification of the manufacturer; and

store the digital fingerprint of the reference physical object in the database.

6. The machine of claim **5**, wherein processor of the digital fingerprint system is further configured to compare the digital fingerprint of the suspect physical object to the digital fingerprint of the reference physical object to generate a result that determines whether the suspect physical object was manufactured in conformance with the specification of the manufacturer;

determine the result indicates a match between the at least one fingerprint feature vector included in the digital fingerprint of suspect physical object and the at least one reference feature vector included in the digital fingerprint of the reference physical object; and

determine the suspect physical object is manufactured in conformance with the specification of the manufacturer based on the match.

7. The machine of claim 1, wherein the fingerprint feature of the suspect physical object includes dimensional qualities associated with at least one physical feature of the suspect physical object.

8. The machine of claim 1, wherein the fingerprint feature of the suspect physical object includes non-alpha-numeric, optically discernible features of the suspect physical object.

9. The machine of claim 1, wherein the fingerprint feature of the suspect physical object includes multiple known indicia of a counterfeit or forged object.

10. The machine of claim 1, wherein the processor of the digital fingerprint system is further configured to parse the image data into the plurality of regions of interest;

collect a piece of region-of-interest data from each region of interest of the image data;

generate identifier data for each region of interest, the identifier data pairing an identifier with the region-of-interest data of a corresponding region of interest; and

associate the identifier data with the digital fingerprint of the suspect physical object.

11. The machine of claim 10, wherein the database includes at least one list of classification elements and individual element values for each of the classification elements, wherein each classification element and its corresponding individual element values together define a corresponding pattern, and wherein the database is arranged to support searching a plurality of patterns for a match based on identifier data associated with digital fingerprints stored in the database.

12. The machine of claim 1, wherein the digital fingerprint of the suspect physical object is based on image data of the portion of the suspect physical object, wherein the image data is independent from identifying information about the suspect physical object included in tags, labels, or other materials added to the suspect physical object.

13. The machine of claim 1, wherein the processor of the digital fingerprint system is further configured to

extract information from the image data;

categorize the extracted information to determine a category; and

include a category indicator in the digital fingerprint of the suspect physical object.

14. The machine of claim 1, wherein the pieces of data of the digital fingerprint of the suspect physical object are responsive to one or more characteristics appearing in a presentable image generated from the image data, the one or more characteristics including a plurality of markings discernible in the presentable image together with respective region data of each of the plurality of markings.

15. The machine of claim 14, wherein the pieces of data of the digital fingerprint of the suspect physical object include size data for each of the plurality of markings.

16. The machine of claim 14, wherein the pieces of data of the digital fingerprint of the suspect physical object include dimension data for each of the plurality of markings, the dimension data defined, at least in part, by corresponding dimensions of each respective marking.

17. The machine of claim 14, wherein the pieces of data of the digital fingerprint of the suspect physical object include pixel-count data for each of the plurality of markings, the pixel-count data defined, at least in part, by a total pixel count of each respective marking.

18. A system comprising:

a processor and memory connected to each other;

a database connected to the processor, wherein the database stores multiple digital fingerprints associated with multiple physical objects;

an input device connected to the processor;

a network interface configured to communicate with the processor and the input device over a network; and

a plurality of lines of instructions stored in the memory and executed by the processor of the system that is configured to

acquire, from the input device, image data of at least a portion of a suspect physical object;

create a digital fingerprint of the suspect physical object based on the image data, wherein the digital fingerprint includes a first piece of data identifying a plurality of regions of interest of the suspect physical object and, for each region of interest, a second piece of data forming at least one fingerprint feature vector that describes a fingerprint feature extracted from the region of interest; and

store the digital fingerprint in the database, wherein the digital fingerprint identifies the suspect physical object as being unique among the multiple physical objects.

19. The system of claim 18, wherein the fingerprint feature includes manufacturing features of the suspect physical object.

20. The system of claim 18, wherein the processor is further configured to acquire, from the input device, image data of at least a portion of a reference physical object that is manufactured according to a specification of a manufacturer;

create a digital fingerprint of the reference object, wherein the digital fingerprint of the reference physical object includes a first piece of data identifying a plurality of regions of interest of the reference physical object and, for each region of interest, a second piece of data forming at least one reference feature vector that describes a fingerprint feature extracted from the region of interest of the reference physical object; and

store the digital fingerprint of the reference physical object in the database.

21. The system of claim 20, wherein the processor is further configured to compare the digital fingerprint of the suspect physical object to the digital fingerprint of the reference physical object to generate a result that determines whether the suspect physical object was manufactured in conformance with the specification of the manufacturer;

determine the result indicates a match between the at least one fingerprint feature vector included in the digital fingerprint of the suspect physical object and the at least one reference feature vector included in the digital fingerprint of the reference physical object; and

determine the suspect physical object is manufactured in conformance with the specification of the manufacturer based on the match.

* * * * *